4. Дорожное яблоко (подбрасывание в общедоступных местах организации (лифт, столовая, парковка) инфицированных носителей информации с мотивирующими к их запуску логотипами/бирками/именами файлов).

После окончания тестирования, специалистами проводится сбор и обработка данных. Часто заказчик хочет знать, кто именно попался на ту, или иную уловку теста. Однако данная информация не передается руководству компании, т.к. проводится тестирование не одного человека, а группы лиц. Соответственно, речь идет об информационной системе, как о едином целом. Исследования показывают, что «человеческий фактор» остается одной из самых распространенных угроз информационной безопасности. Для снижения рисков, связанных с этим обстоятельством, используются различные технические и административные механизмы защиты. Один из них – повышение осведомленности работников, в области информационной безопасности.

ВЫСОКОПРОИЗВОДИТЕЛЬНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ХЭШ-ФУНКЦИИ SHA-256 НА БАЗЕ FPGA

М.В. Качинский, А.В. Станкевич

Криптографическая хэш-функция SHA-256 описана в документе RFC 4634 [1] и предназначена для получения хэш-значения фиксированной длины для входного сообщения произвольной длины. Данная функция используется в различных приложениях, связанных с защитой информации, а также в большинстве криптовалют. В указанных приложениях возникает необходимость высокопроизводительных аппаратных реализаций SHA-256. В докладе рассматривается полностью конвейерная реализация хэш-функции SHA-256 для одного блока данных (512 бит) на базе FPGA.

Характерной особенностью алгоритма SHA-256 является длинная цепочка последовательных сложений при вычислении новых значений переменных A и E. Для уменьшения числа сложений в одном такте реализации и, следовательно, повышения тактовой частоты конвейерного процессора вычисление переменных E-H на такт опережает вычисление переменных A-D. Кроме того используется предварительное вычисление сумм W_t, K_t, H и D. Одна ступень конвейерного процессора производит вычисления за один такт частоты синхронизации. Общее число ступеней конвейера с учетом 64 раундов алгоритма SHA-256 и завершающего сложения со значением вектора инициализации равно 67.

Характеристики реализации по отчету средств синтеза пакета ISE 14.7 для кристалла FPGA семейства Kintex7 XC7K160T-3: 27477 триггеров секций, 35161 просмотровая таблица (LUT), тактовая частота – 352 МГц.

При обработке сообщения, длина которого превышает один блок SHA-256 необходимо либо последовательно включить требуемое число процессорных ядер для реализации полностью конвейерного вычислителя, либо организовать итеративные вычисления на одном процессорном ядре, коммутируя с помощью мультиплексора выходные данные процессора на его вход требуемое число раз.

Литература

1. RFC 4634. US Secure Hash Algorithms (SHA and HMAC-SHA). [Электронный ресурс]. – URL: https://tools.ietf.org/pdf/rfc4634.pdf (дата обращения: 26.04.2018).

ДОСТУП К ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Р.В. Кислинский

Под информацией ограниченного распространения в Республике Беларусь понимаются государственные секреты, т. е. сведения, защищаемые государством в целях предотвращения их несанкционированного распространения и создания угрозы национальной безопасности Республики Беларусь, а также конституционным правам и свободам граждан.

Что касается перечня сведений, составляющих государственные секреты Республики Беларусь, то он определен как совокупность категорий сведений в области экономики,

политики, экологии, оперативно-розыскной деятельности, военной сфере и других жизненно важных сферах деятельности, несанкционированное распространение которых создает или может создать угрозу национальной безопасности Республики Беларусь, а также конституционным правам и свободам граждан. Существенной мерой защиты государственных секретов является порядок допуска к ним лиц, которым она необходима для выполнения соответствующих функций. Прежде всего, этот порядок регламентируется Законом Республики Беларусь «О государственных секретах» и Положением о порядке предоставления допуска физическим лицам к государственным секретам, утвержденном Постановлением Совета министров Республики Беларусь 10 апреля 2004 года № 400. Закон «О государственных секретах» ограничивает возможность физических лиц, не достигших восемнадцатилетнего возраста, на доступ к государственным секретам со степенями секретности особой важности и совершенно секретно, за исключением лиц, достигших семнадцатилетнего возраста и поступивших в учебные заведения, где для обучения необходим доступ к государственным секретам.

Цель принятия различных мер по защите информации – обеспечить такой режим работы с информацией, при котором доступом к информации будут иметь только имеющие соответствующий уровень доступа.

Литература

1. Постановление Совета министров Республики Беларусь «Об утверждении положения о порядке предоставления допуска физическим лицам к государственным секретам» 10 апреля 2004 г. № 400.

2. Закон Республики Беларусь от 19.07.2010 г. № 170-З «О государственных секретах».

ВОПРОСЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ВОЕННЫХ ГОРОДКОВ

А.Н. Коваленко

Для каждого военного городка должна разрабатываться, на основе общих требований, своя собственная система безопасности, исходя из положений которой, разрабатывается проект оснащения объекта инженерно-техническими средствами охраны, специальными и программно-аппаратными средствами защиты. Для решения задач и проблем выбора структуры и состава комплекса инженерно-технических средств охраны необходимо, проанализировать возможные варианты действий нарушителя. Исходя из анализа возможных действий нарушителя, составляются варианты его моделей, которые и принимаются за основополагающий фактор выбора тактики защиты объекта.

При разработке проекта оборудования инженерно-техническими средствами охраны военных городков, помимо гаммы технических факторов, необходимо учитывать факторы, определяемые поведением нарушителя.

Возможность нарушителя найти маршрут, не блокированный средством обнаружения, должна быть исключена. Для предотвращения прохода нарушителя должны быть блокированы все возможные маршруты движения нарушителя. Состояние физических преград, имеющих большую стойкость и в связи с этим не блокированных средствами обнаружения, должно периодически контролироваться патрулями или системой видеонаблюдения.

Для увеличения вероятности обнаружения подготовленного и технически оснащенного нарушителя, организовываются полностью скрытные рубежи охраны. Для предотвращения возможности имитации работы средств обнаружения, соединительные линии системы сбора, обработки и отображения информации должны иметь физическую и сигнализационную защиту коммутационных шкафов, коробок и т.п. При прокладке кабелей предпочтение следует отдавать скрытой проводке в закладных устройствах, обеспечивающих дополнительное экранирование и инженерную защиту. Правильный выбор системы и способа охраны и своевременность действий должностных лиц обеспечит надежную охрану объектов военного городка.

Литература

1. Гарсиа, М. Л. Проектирование и оценка систем физической защиты. М.: АСТ, 2003. 386 с.

2. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения. М.: Горячая линия – Телеком, 2004. 367 с.