ИСПОЛЬЗОВАНИЕ ПО SECRET NET ДЛЯ АВТОМАТИЗАЦИИ КОНТРОЛЯ ЦЕЛОСТНОСТИ ФАЙЛОВ ПРОВЕРКОЙ ИХ КОНТРОЛЬНЫХ СУММ

Е. В. Дмитриева, Т. Ю. Серова, Ю. В. Зверьков, М. М. Захаров, И. Л. Бондарь

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

Введение

Неотъемлемой частью технических мер по защите информации, принимаемых в государственных информационных системах (далее – ГИС), является обеспечение целостности как компонентов ГИС, так и информации, обрабатываемой в ней.

В целях обеспечения защиты от несанкционированного доступа, копирования, предоставления, распространения, уничтожения, модифицирования, блокирования, а также от других неправомерных действий в отношении обрабатываемых данных в ГИС применяются программные или аппаратно-программные средства защиты информации (далее – СрЗИ), имеющие необходимые функции безопасности.

В соответствии с требованиями нормативных документов регуляторов Российской Федерации в области информационной безопасности [1, 2], в ГИС должна быть обеспечена целостность программного обеспечения (далее – ПО), включая программное обеспечение средств защиты информации (мера ОЦЛ.1). Поэтому отсутствие любых несанкционированных изменений в прикладных программных продуктах, а особенно в средствах защиты информации, является важным условием обеспечения информационной безопасности ГИС в целом.

Контроль целостности

Согласно документам [2, 3], целостность информации – это состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Согласно документу [4] под целостностью информации понимается способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и(или) непреднамеренного искажения (разрушения).

Для своевременного обнаружения модификации ресурсов системы предназначен механизм контроля целостности, позволяющий обеспечить корректность ее функционирования и целостность обрабатываемой в ней информации.

Как правило, механизм контроля целостности реализуется разработчиками средств защиты информации от несанкционированного доступа. В основе механизма лежит проверка соответствия контролируемого ресурса системы (файла каталога, элемента реестра ОС Windows) эталонному значению. Периодичность контроля ресурсов задается во время настройки механизма с возможностью выбора реакции системы защиты на обнаружение несоответствия.

Наиболее часто встречающимися в средствах защиты информации методами проверки целостности данных являются:

– полная копия данных;
– контрольная сумма;
– имитовставка;
– хэш;
– электронная подпись.

Полная копия данных – это дополнительная копия данных для последующей сверки. Данный метод прост в реализации и предусматривает полноценный контроль данных.

Контрольная сумма – это некоторое значение, рассчитанное по набору данных путем применения определенного алгоритма. Самым известным алгоритмом нахождения контрольной суммы для проверки целостности данных является «циклический избыточный код (cyclic redundancy code, CRC)», который основан на свойствах деления с остатком двоичных многочленов. Остатком от деления многочлена, соответствующего входным данным, на некоторый заранее известный делитель (полином) является значением контрольной суммы. Важной характеристикой вычисления контрольной суммы является степень полинома – действительная позиция старшего бита, обычно это степень 8, 16 или 32, так как они являются кратными разрядности регистров современных процессоров, что значительно упрощает реализацию алгоритмов CRC (CRC-8, CRC-16, CRC-32).

Имитовставка – это некоторое значение фиксированной длины, полученное по определенному правилу из открытых данных и закрытого ключа. Значение имитовставки добавляется к зашифрованным данным для обеспечения защиты от навязывания ложных данных. Вычисление имитовставки предусмотрено в алгоритме ГОСТ 28147-89 в соответствующем режиме. Длина имитовставки от 1 до 32 бит. Для ее вычисления открытые данные представляют в виде последовательности блоков длиной 64 бита. Последний блок при необходимости дополняется нулями до полного 64-разрядного блока. Первый блок открытых данных подвергают преобразованию, соответствующему первым 16 циклам алгоритма шифрования в режиме простой замены ГОСТ 28147-89.

В качестве ключа для выработки имитовставки используют ключ длиной 256 бит, по которому шифруют данные. Полученное после 16 циклов 64-разрядное число суммируют по модулю 2 со вторым блоком открытых данных. Результат суммирования снова подвергают преобразованию. Полученное 64-разрядное число суммируют по модулю 2 с третьим блоком открытых данных и снова подвергают преобразованию, получая 64-разрядное число и т. д. Последний блок суммируют по модулю 2 с результатом вычислений на предпоследнем шаге, после чего зашифровывают в режиме простой замены, используя криптографическое преобразование. Первые 32 бита получившегося блока составляют имитовставку. Спецификация ГОСТ 28147-89 предусматривает использование в качестве имитовставки и меньшее количество бит, но не большее.

Хэш – это некоторое значение, полученное в результате обработки неких данных хэш- функцией, которая осуществляет необратимое преобразование массива входных данных произвольной длины в битовую (выходную) строку фиксированной длины, выполняемое определенным алгоритмом. Отечественным стандартом генерирования хэш-функций является алгоритм ГОСТ Р 34.11-2012. Этот стандарт разработан и введен в качестве замены устаревшему алгоритму ГОСТ Р 34.11-94. На вход хеш-функции подаются данные произвольного размера. Далее они разбиваются на блоки по 512 бит, если размер данных не кратен 512, то блок дополняется необходимым количеством бит. Потом итерационно используется функция сжатия, в результате действия которой обновляется внутреннее состояние хеш-функции. Также вычисляется контрольная сумма блоков и число обработанных бит. Когда обработаны все блоки исходных данных, производятся еще два вычисления: обработка функцией сжатия блока с общей длиной данных и блока с контрольной суммой. Они и завершают вычисление хеш-функции.

Электронная подпись – это некоторое зашифрованное значение вычисленного хэша по входным данным. Принцип работы электронной подписи заключается в следующем: первым шагом является вычисление значения хэш-функции на основе входных данных (файла), в результате чего получается хэш. Затем полученный хэш шифруется с помощью закрытого ключа для получения подписи файла. При вычислении значения хэш-функции также используется алгоритм ГОСТ Р 34.11-2012.

Каждый из перечисленных методов проверки целостности данных имеет как преимущества, так и недостатки. Все вычисляемые значения (CRC, хэш, имитовставка, электронная подпись) имеют малый размер, используемые для их вычисления криптографические алгоритмы, за исключением CRC, являются криптостойкими, т. е. подобрать исходные данные к заранее известному значению за приемлемое время невозможно. При этом, для одного значения может существовать множество исходных данных. Копии данных, а также значения CRC, хэша можно подменить. Использование закрытого ключа в алгоритмах выработки имитовставки и электронной подписи исключают подмену значений. Благодаря простоте и скорости реализации, методы «полная копия данных» и «контрольная сумма» имеют широкое применение, несмотря на их полную криптографическую незащищенность. Помимо того, что перечисленные методы контроля реализуются в средствах защиты в виде отдельного механизма, алгоритмы, применяемые в этих методах, широко используются для подсчета контрольных сумм программных модулей с фиксированием и отображением результатов контрольного суммирования.

Программы контроля целостности

Контроль целостности программного обеспечения – это обнаружение любых модификаций программных модулей.

Дистрибутив программного обеспечения содержит установочный комплект программы для начальной инициализации и может быть приобретен у производителя или у официального дилера на материальном носителе или скачан с официального сайта производителя.

При получении дистрибутива ПО необходимо убедиться в целостности полученных данных. Для этого на сайте производителя или, в случае сертифицированного ПО (средство защиты информации), в документации (формуляре) на него указываются контрольные суммы оригинальных установочных файлов, а также название программы и алгоритм для выполнения контрольного суммирования, чтобы получить достоверные результаты. Если значения контрольных сумм дистрибутива совпадут со значениями, представленными производителем, это будет являться гарантией его защиты от подмены.

Согласно требованиям нормативного документа [2] в ГИС должен быть предусмотрен контроль целостности по наличию имен и (или) по контрольным суммам программного обеспечения. Для программного обеспечения средств защиты информации контроль целостности должен осуществляться по контрольным суммам всех компонентов средств защиты, как в процессе загрузки, так и динамически в процессе работы системы. При условии приобретения сертифицированного ПО помимо указанных в формуляре контрольных сумм дистрибутива, в нем также приводятся контрольные значения установленных программных модулей. Поэтому, после его установки на ПЭВМ, необходимо выполнить расчет контрольных сумм программой, заявленной производителем ПО, и сравнить полученные значения контрольных сумм со значениями из формуляра. Данная проверка регламентирована в ГОСТ РО 0043-004-2013 [5] и проводится при вводе ГИС в эксплуатацию.

Как было сказано выше, для проверки целостности программного обеспечения существуют различные программы, утилиты и комплексы, реализующие алгоритмы шифрования.

Одной из таких программ является утилита *cpverify.exe*, разработанная компанией ООО «КРИПТО-ПРО». Утилита осуществляет проверку целостности файлов, контрольные суммы которых рассчитываются в соответствии с ГОСТ Р 34.11-2012.

Еще одной программой для подсчета контрольных сумм файлов является *csum-2012.exe* компании ООО «Код безопасности». Программа работает по алгоритму ГОСТ 28149-89 в режиме выработки имитовставки.

Наиболее частой программой, используемой разработчиками средств защиты информации для расчета и проверки контрольных сумм, является *программа фиксации и контроля исходного состояния программного комплекса «ФИКС»*, разработанная организацией ООО «Центр безопасности информации». Программа производит вычисление контрольных сумм заданных файлов по одному из пяти реализованных алгоритмов, в том числе в соответствии с ГОСТ Р 34.11-94, и имеет сертификат соответствия по второму уровню контроля отсутствия недекларированных возможностей, выданный ФСТЭК России, что позволяет использовать ее в защищенных ГИС.

Все эти программы выполняются автономно на ПЭВМ, поэтому одновременное проведение проверки на большом количестве компьютеров трудозатратно и малоэффективно. Таким образом, используя возможности средств защиты со встроенным механизмом контроля целостности, можно автоматизировать процесс проверки контрольных сумм.

Механизм контроля целостности Secret Net

Средство защиты информации от несанкционированного доступа Secret Net предназначено для обеспечения безопасности информационных систем на компьютерах, функционирующих под управлением ОС семейства Microsoft Windows.

Одной из основных защитных функций Secret Net является контроль целостности файловых объектов и реестра. В сетевом варианте исполнения Secret Net в централизованном хранилище создана база данных контроля целостности, содержащая две модели данных – для компьютеров под управлением 32- и 64-разрядных версий ОС Windows, соответственно. Каждая модель данных связана с субъектами управления – группами безопасности Active Directory, созданными во время развертывания Secret Net в домене. Данные субъекты по умолчанию содержат задания контроля целостности ПО СрЗИ Secret Net, реестра и файлов ОС Windows, выполнение проверки по которым осуществляется по содержимому ресурсов с помощью алгоритма CRC. Поскольку встроенная проверка, основанная на данном алгоритме, приводит к инцидентам информационной безопасности, связанным с нарушением целостности ресурсов (ввиду «несовершенства» алгоритма CRC), для большей достоверности результатов проверки в дополнение к существующему методу контроля предлагается использовать метод проверки, основанный на алгоритме «полное совпадение».

Решение, представленное в докладе, описывает способ полной проверки файлов контролируемого программного обеспечения, с файлами, контрольные суммы которых проверены специализированной программой контроля целостности и совпадают со значениями в формуляре.

Этапы реализации решения по контролю целостности

Таким образом, внедрение решения по контролю целостности файлов проверкой их контрольных сумм, можно разбить на следующие этапы:

– выбор программного продукта, нарушение целостности которого является критическим;

– проверка целостности полученного дистрибутива ПО;

– выделение «эталонной» ПЭВМ для установки ПО, подлежащего проверке;

– инсталляция программного обеспечения на «эталонную» ПЭВМ с определением состава ПО и расположения в зависимости от разрядности операционной системы;

– расчет и проверка контрольных сумм установленного ПО на «эталонной» ПЭВМ;

– настройка механизма контроля целостности;

– инсталляция программного обеспечения, подлежащего проверке, на компьютеры и серверы ГИС;

– добавление учетных записей компьютеров и серверов в соответствующие группы безопасности.

При выборе программного продукта для контроля необходимо оценить насколько нарушение его целостности будет являться критическим. Чаще всего нарушение целостности программных модулей средств защиты информации является потенциальной уязвимостью информационных систем. Поэтому, в основе представленного в докладе решения лежит процесс автоматизации проверки контрольных сумм именно файлов средств защиты информации.

Определившись с ПО, которое необходимо контролировать, проверяется целостность полученного дистрибутива. В случае совпадения контрольных сумм дистрибутива со значениями, представленными производителем в формуляре, можно сделать вывод, что установочный комплект получен из доверенного источника и можно перейти к этапу его установки.

Перед установкой ПО СрЗИ на рабочие станции и серверы ГИС, необходимо определить все используемые в ГИС операционные системы. На основании полученных данных в состав домена вводятся новые «эталонные» компьютеры и серверы под управлением всех найденных в ГИС версий ОС с учетом их разрядности. На каждой «эталонной» ПЭВМ выполняется установка ПО СрЗИ. Ввиду того, что ГИС может иметь особенности функционирования и утвержденную политику безопасности, функционал устанавливаемого ПО СрЗИ может быть задействован не в полном объеме. На этапе инсталляции происходит конкретизация параметров установки ПО СрЗИ, а также выбор места размещения ПО, которое

будет указываться в дальнейшем во время его развертывания на компьютерах и серверах ГИС. Поскольку данные компьютеры и серверы содержат «эталонные» установки ПО СрЗИ, к ним обеспечивается доступ только административному персоналу ГИС.

Далее выполняется расчет контрольных сумм файлов установленного программного обеспечения средств защиты на всех «эталонных» ПЭВМ, результаты контрольного суммирования каждого фиксируются документально.

Следующим этапом выполняется настройка контроля целостности. Для этого в каталоге Active Directory для выбранного ПО СрЗИ с учетом его версии и разрядности используемой ОС создаются соответствующие группы безопасности. Они предназначены для дальнейшего включения в них учетных записей компьютеров и северов, подлежащих проверке целостности. Состав групп контролируется, информация о любых изменениях фиксируется в журнале безопасности ОС Windows и поступает в базу данных сервера безопасности Secret Net. В программе настройки механизма контроля целостности Secret Net созданные группы безопасности добавляются в качестве субъектов управления. Для каждого субъекта создается задание контроля целостности, в которое включаются файлы соответствующего ПО СрЗИ. Задается вид задания – «тиражируемое», т. е. эталонные значения будут рассчитаны централизованно и храниться в базе данных контроля пцелостности. В качестве алгоритма выбирается – «полное совпадение». Это значит, что эталонным значением для контроля будет являться копия ресурса, контрольная сумма которого вычислена и совпадает со значением, указанном в формуляре. Для соблюдения требований документа [2] в части периодичности контроля целостности, для задания настраивается расписание таким образом, чтобы проверка осуществлялась во время загрузки и динамически в процессе работы системы. Включение файлов ПО СрЗИ в задание контроля целостности происходит на «эталонной» ПЭВМ, версии ОС и СрЗИ которых соответствуют названию задания. После сделанных изменений в базе данных контроля целостности эталонные значения ресурсов сохраняются в централизованном хранилище.

Поскольку проверка выполняется посредством ПО Secret Net, клиентская часть данного программного продукта должна быть установлена на всех планируемых к проверке компьютерах и серверах ГИС.

После выполненных действий по настройке механизма, проверяемое ПО СрЗИ устанавливается на компьютеры и серверы ГИС в заранее определенный каталог, и по завершении установки его учетная запись включается в соответствующую группу безопасности Active Directory. После перезагрузки компьютера и сервера эталонные значения рассчитанных ресурсов тиражируемых заданий контроля целостности распространятся на них.

Успешное выполнение задания контроля целостности свидетельствует об использовании на компьютере и сервере подлинного ПО СрЗИ, контрольные суммы файлов которого соответствуют эталонным значениям.

При обнаружении несоответствия контролируемого файла эталонному в журнале Secret Net фиксируется событие о нарушении целостности ресурса, которое передается на хранение в базу данных сервера безопасности. В качестве реакции системы защиты на возникновение подобного инцидента можно выбрать параметр «заблокировать компьютер». По окончании проведения анализа ситуации и восстановления файлов ПО СрЗИ с корректными значениями контрольных сумм блокировка ПЭВМ снимается административным персоналом.

Обновление контролируемого ПО потребует создания дополнительных заданий контроля целостности, повторяя весь процесс внедрения решения с самого начала. Это влечет за собой увеличение объема базы данных контроля целостности за счет добавления в нее копий оригинальных файлов обновленного ПО.

Заключение

Внедрение решения позволяет исключить необходимость проверки контрольных сумм сертифицированного ПО на каждом компьютере и сервере ГИС. Автоматизация контроля целостности файлов проверкой их контрольных сумм позволяет повысить качество проверки за счет отсутствия «человеческого» фактора, ее достоверность, а также существенно снизить трудозатраты административного персонала.

Данное решение позволяет проводить проверку подлинности используемого ПО централизованно на регулярной основе и гарантирует использование только тех программных продуктов, контрольные суммы файлов которых соответствуют эталонным значениям.

Решение успешно внедрено и применяется в двух автоматизированных системах ФГУП «РФЯЦ-ВНИИЭФ».

Литература

1. Приказ ФСТЭК России «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 № 17.

2. Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» от 11 февраля 2014 г.

3. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

4. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» от 30 марта 1992 г.

5. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний.