УДК 004.056.57

Метод экспресс-анализа событий, связанных с воздействиями на файлы, предназначенный для расследования инцидентов информационной безопасности

Н. А. Гайдамакин, Р. В. Гибилинда, Н. И. Синадский

В статье предложен метод экспресс-анализа событий информационной безопасности (ИБ), основанный на представлении инцидента как совокупности событий, состоящих из воздействий на файлы. Метод предполагает применение базы данных шаблонов идентифицированных воздействий, исходными данными для которых являются записи журнала изменений тома файловой системы NTFS – $UsnJrnl. Рассмотрен алгоритм поиска и классификации воздействий на файлы с использованием шаблонов. Предлагаемый метод экспресс-анализа позволяет определить порядок событий в рамках расследуемого инцидента ИБ, сократив количество анализируемых массивов данных до одного – журнала $UsnJrnl.

Ключевые слова: расследование инцидентов информационной безопасности, событие информационной безопасности, воздействие на файл, шаблон воздействия на файл.

1. Введение

Менеджмент инцидентов, являющийся важной составляющей управления информационной безопасностью (ИБ), включает в первую очередь расследование инцидентов в целях выяснения и устранения их причин и условий, им способствующих. В соответствии с [1, п. 3.2.7] инцидент информационной безопасности определяется как «любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность». Причинами, способствующими возникновению инцидентов ИБ, являются как компьютерные атаки (согласно [2] компьютерная атака – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы[1] или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств), так и действия пользователя, нарушающие действующую политику безопасности, принятую в организации.

Таким образом, процесс расследования инцидентов ИБ включает, прежде всего, анализ событий («определённой совокупности обстоятельств» [1, п. 3.2.8]), являющихся в соответствии с [4] составляющими частями инцидента ИБ. К ключевым событиям относятся те, которые связаны с воздействиями на файлы, содержащими защищаемую информацию.

Под воздействием на файлы понимается совокупность файловых операций[2], связанных по назначению, разделённых по времени и приводящих к изменению характеризующих признаков одного или нескольких файлов [5]. При этом следует отметить, что в процессе обработки

[1] Информационная система – система, организующая обработку информации о предметной области и её хранение [3].

[2] Под файловой операцией понимается процесс модификации значений признаков (параметров), характеризующих файл.

информации в компьютерной системе[3] (КС), являющейся основой информационной системы (ИС), осуществляется множество файловых операций.

С одной стороны, файловые операции, являющиеся результатом обработки информации пользователем КС, можно трактовать как санкционированные воздействия на файлы, т.е. не приводящие к нарушениям ИБ. С другой стороны, сценарии и технологии реализации компьютерных атак могут включать в том числе различные файловые операции, совокупность которых может составлять воздействия на файлы, аналогичные осуществляемым в ходе пользовательской обработки информации. Однако такие воздействия, называемые несанкционированными, характеризуются другими субъектами, т.н. злоумышленниками, и/или направлены на нарушение ИБ и/или создание условий для её нарушения.

В результате при расследовании инцидентов ИБ необходимо рассматривать и анализировать события, связанные как с санкционированными, так и с несанкционированными воздействиями на файлы, чтобы выделить и идентифицировать[4] те из них, которые непосредственно связаны с инцидентом. Общее количество событий, связанных с воздействиями на файлы, зависит от нескольких факторов, таких как: количество файлов, активность пользователя в работе с файлами, тип действий злоумышленника (использование вредоносного программного обеспечения, внедрение уязвимостей в сервисы КС с целью получения контроля над ней), решаемые КС задачи и др. Рассмотрим два примера, которые описывают зависимость количества событий от ранее указанных факторов.

Первым примером является использование злоумышленником на компьютере жертвы вредоносного программного обеспечения Jigsaw [6], предназначенного для шифрования содержимого пользовательских файлов с целью последующего «вымогания» денежных средств за ключ расшифрования. При наличии 100 файлов, владельцем которых является пользователь, Jigsaw в процессе своей работы создаст 150–200 событий, связанных с воздействиями на файлы. Количество же санкционированных воздействий, обусловленных активностью пользователя в период работы Jigsaw, зачастую не превышает 10–15.

Второй пример – внедрение кода в Web-приложение. Пусть Web-сервер в процессе своей работы осуществляет 20000 событий, связанных с воздействиями на файлы, в час. Основной файловой операцией, выполняемой Web-сервером при обработке запросов, является чтение файлов, в которых содержится исходный код Web-приложений. Злоумышленник, реализуя компьютерную атаку типа «внедрение кода», изменяет содержимое Web-приложения, формирующего страницу сайта, где пользователь может изменить пароль от своей учетной записи. В данном случае цель злоумышленника – кража учетных данных. В результате формируются 1–2 события, связанные с изменением содержимого файла.

Как видно из примеров, работа специалиста-аналитика по расследованию инцидента ИБ осложняется тем, что ему необходимо идентифицировать и классифицировать заранее неизвестное количество событий, связанных с воздействиями на файлы.

Одним из направлений разрешения указанной проблемы является разделение процесса анализа событий, связанных с воздействиями на файлы, на т.н. экспресс-анализ[5] и в случае необходимости дальнейшее детальное исследование специалистом-аналитиком, проводящим расследование. Разработанный метод экспресс-анализа событий, основанный на использовании массивов данных, содержащих информацию о воздействиях на файлы, отличается от известных методов [7–9] использованием шаблонов[6] с целью последующей идентификации и классификации воздействий.

---

[3] Совокупность аппаратных средств, управляемых программным обеспечением (операционной системой) как единый модуль [3].

[4] Под идентификацией воздействия на файл в рамках статьи будем понимать процесс определения действия, совершённого по отношению к файлу, на основе анализа значений признаков, его характеризующих.

[5] Анализ, целью которого является составление перечня событий, связанных с воздействиями на файлы и классифицированных как несанкционированные, с указанием времени события и его типа.

[6] Под шаблоном воздействия на файл понимается декомпозиция данных, характеризующая это воздействие и позволяющая выделить его среди множества остальных воздействий.

2. Общая схема метода экспресс-анализа событий ИБ

КС работают под управлением многозадачных систем, вследствие чего специалист-аналитик, как уже отмечалось, вынужден исследовать множество как санкционированных, так и несанкционированных воздействий на файлы, «сплетённых» в едином массиве данных. Для сокращения объёма анализируемой информации необходимо разделить (классифицировать) множество осуществлённых воздействий на нормальные, условно аномальные (предварительно – «подозрительно» аномальные) и аномальные. Нормальные воздействия не имеют отношения к инциденту ИБ и должны быть исключены из отчёта специалистом-аналитиком, проводящим расследование. Условно аномальные воздействия должны быть рассмотрены в рамках инцидента в том случае, если удовлетворяют дополнительным критериям, например, дата и время начала/окончания, расположение файлов и т.д. Аномальные воздействия, которые не должны возникать в процессе штатного функционирования КС, должны быть проанализированы в приоритетном порядке.

Установление взаимосвязи между классифицированным воздействием на файл и событием ИБ осуществляется следующим образом. В соответствии с [3] инцидент ИБ Q определяется как совокупность событий ИБ и описывается выражением:

$$Q = \left\{ \left\langle S_1, ..., S_p \right\rangle \right\}, \tag{1}$$

где $S_1, ..., S_p$ – события ИБ, а p – их количество. В работе [4] каждое событие ИБ рассматривается с позиции воздействий на файлы и описывается выражением:

$$S_k = \left\langle \left\langle A_{ji}^k \right\rangle_{i=1}^{l} \right\rangle_{j=1}^{n}, \tag{2}$$

где A_{ji}^k – воздействие i на файл j, относящееся к событию ИБ k; l – количество воздействий; n – количество файлов.

Таким образом, в соответствии с (1) и (2) инцидент ИБ состоит из событий, а события ИБ представляются совокупностью воздействий на файлы. Следовательно, на основе классификации воздействий на файлы специалист имеет возможность выявлять связанное событие ИБ.

Предлагаемый метод экспресс-анализа нацелен на автоматизированное определение порядка возникновения событий ИБ за счёт использования шаблонов воздействий на файлы и состоит из двух этапов. На первом (подготовительном) этапе на основе идентифицированных воздействий на файлы необходимо подготовить шаблоны воздействий, оценив их аномальность применительно к процессу штатной обработки информации в исследуемой КС, и сформировать базу данных шаблонов. Второй этап (расследование инцидента ИБ) заключается в осуществлении поиска и классификации воздействий на файлы с применением подготовленной базы данных шаблонов. Метод позволяет сконцентрировать внимание специалиста только на тех событиях ИБ, которые связаны с несанкционированными воздействиями на файлы.

3. Поиск и классификация воздействий на файлы с применением подготовленной базы данных шаблонов

Содержащиеся в базе шаблоны должны быть структурированы в соответствии с задачами, решаемыми узлом инфраструктуры ИС. Так, например, на Web-сервере уделяется особое внимание файлам Web-приложений, файлам конфигурации сервисов, изображениям, видео, текстовым файлам, используемым непосредственно для работы Web-ресурса.

3.1. Идентификация воздействий на файлы

В рамках реализации предлагаемого метода экспресс-анализа событий ИБ разработано программное средство, которое осуществляет автоматизированный процесс идентификации воздействий на файлы на основе предварительно подготовленных шаблонов воздействий с отмеченными признаками нормальности, условной и безусловной аномальности. Анализ воздействий на файлы производится по данным журнала изменений тома файловой системы NTFS $UsnJrnl [10] (далее – журнал).

На рис. 1 представлен пример идентификации и классификации по признаку аномальности воздействий на файлы при помощи разработанного программного средства в рамках эксперимента, в ходе которого на компьютерную систему осуществлялась атака типа «внедрение кода», направленная на нарушение конфиденциальности и целостности исходного кода Web-приложений, послужившая причиной инцидента ИБ.

Сигналом об обнаружении атаки является сработка системы обнаружения атак. Из данных о сработке специалист, который начинает расследование инцидента ИБ, получает время атаки, её тип и IP-адрес узла, которые подаются на вход программного средства экспресс-анализа для установления условий аномальности воздействий на файл.

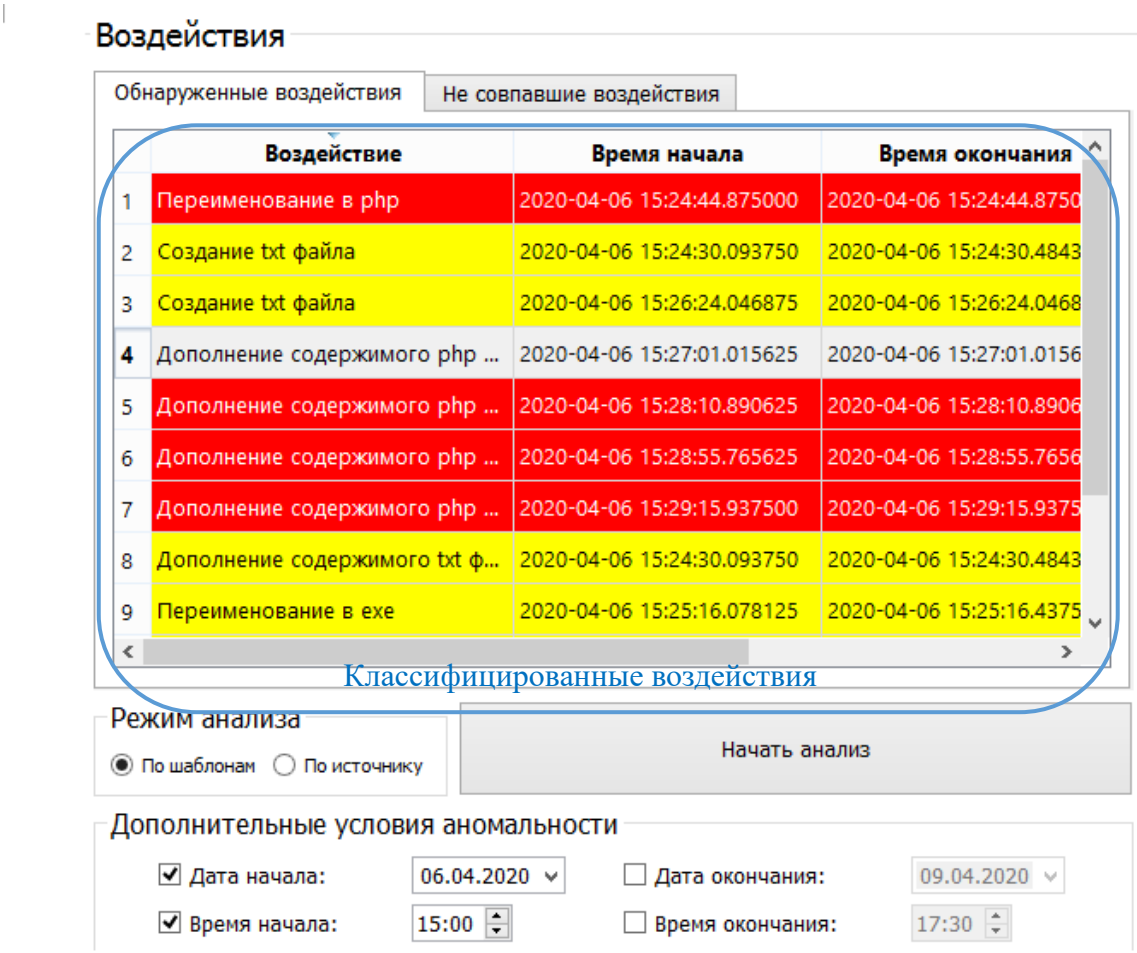

Рис. 1. Классификация воздействий на файлы с применением шаблонов

На рис. 1 красным цветом выделены идентифицированные аномальные воздействия на файлы, желтым цветом – условно аномальные воздействия, которые удовлетворяют дате и времени начала инцидента ИБ. В примере идентифицировано воздействие компьютерной атаки типа «внедрение кода», в процессе которой осуществляется переименование файла с расширением *.php.

Полученный результат достигается специалистом-аналитиком на основе ранее подготовленной базы данных шаблонов и последующего её применения для поиска и классификации воздействий в рамках расследования.

3.2. Подготовка базы данных шаблонов воздействий на файлы

Обладая знаниями об используемых в КС технологиях (версия операционной системы, тип прикладного программного обеспечения), специалист-аналитик заранее готовит базу данных, содержащую шаблоны типовых воздействий на файлы.

Источником информации о воздействиях на файлы является, как уже отмечалось, журнал. Структуру журнала составляют записи, формат которых представлен в табл. 1. Поля, отмеченные курсивом, используются при идентификации воздействий на файлы.

Таблица 1. Формат записи журнала изменений тома $UsnJrnl

Смещение, байт	Размер, байт	Описание поля
0x00	4	Размер записи
0x04	2	Версия записи
0x06	2	Версия программного обеспечения, которым запись создана
0x08	8	*Идентификатор файловой записи*
0x10	8	*Идентификатор родительского каталога*
0x18	8	*Номер записи*
0x20	8	*Временная отметка создания записи*
0x28	4	*Идентификатор операции*
0x2C	4	Тип источника записи
0x30	4	Идентификатор безопасности
0x34	4	Атрибуты файла
0x38	2	Длина имени файла *
0x3A	2	Начало имени файла в записи
0x3C	*	*Имя файла*

Примеры некоторых значений поля «Идентификатор операции» [10], которые были проанализированы в рамках проведенного эксперимента, представлены в табл. 2.

Таблица 2. Примеры значений поля «Идентификатор операции»

Значение поля (в десятичной системе счисления)	Описание
1	Содержимое файла перезаписано
2	Содержимое файла дополнено
4	Содержимое файла уменьшено
256	Создание файла
512	Удаление файла
4096	Предыдущее имя файла
8192	Новое имя файла
32768	Изменение служебной информации о файле
2147483648	Закрытие файла

Значения полей записей журнала являются основой шаблона G, который представляет собой совокупность фиксированных значений, описываемых вектором:

$$G = \{\langle G_{name}, G_{anomaly}\rangle, \langle I_G, I_{sign}\rangle, \langle D_G, D_{sign}\rangle, \langle N_G, N_{sign}\rangle, \langle R_G, R_{sign}\rangle\}, \quad (3)$$

где в отношении к рассматриваемому шаблону воздействия:

- G_{name} – название шаблона воздействия;
- $G_{anomaly}$ – признак аномальности воздействия;
- I_G – множество значений, описывающих идентификаторы файловых записей[7];
- D_G – множество значений, описывающих идентификаторы родительских каталогов[8];
- N_G – множество значений, описывающих имена файлов[9], расширения имен файлов и используемые специальные символы[10] (при их наличии);
- R_G – множество значений, описывающих идентификаторы операций, полученных из поля «Идентификатор операции» (табл. 1) записей журнала;
- I_{sign}, D_{sign}, N_{sign}, R_{sign} – признаки значимости соответствующих множеств значений I_G, D_G, N_G, R_G для воздействия на файл, описываемого шаблоном G.

На рис. 2 показан пример генерации шаблона (нижняя таблица рис. 2), соответствующего идентифицированному воздействию на файл (верхняя таблица рис. 2) – замена расширения файла с txt на php (переименование), в результате чего интерпретатор PHP будет выполнять программный код, содержащийся в файле.

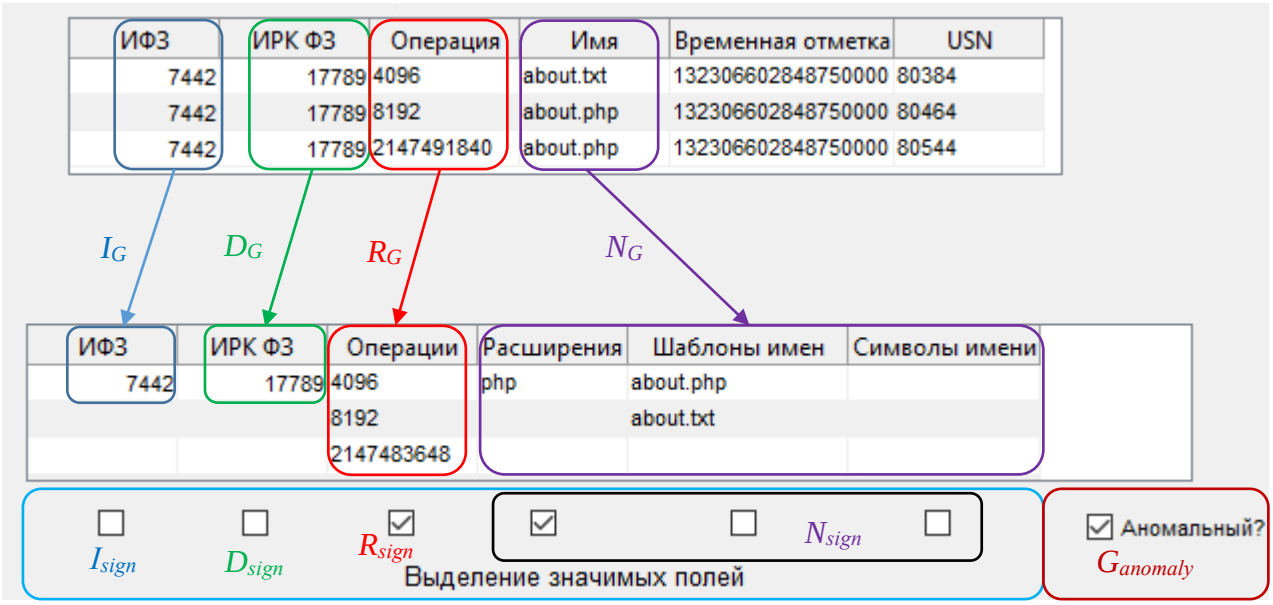

Рис. 2. Пример генерации шаблона воздействия –
замена расширения файла с txt на php в целях осуществления атаки типа «внедрение кода»

На рисунке столбцы таблиц соответствуют следующим полям записей журнала (табл. 1) и компонентам вектора G:

- «ИФЗ» – идентификаторы файловых записей I_G;
- «ИРК ФЗ» – идентификатор родительских каталогов, принадлежащих D_G;

[7] Идентификатор файловой записи – уникальное числовое значение, содержащееся в служебной информации о файле, используемое драйвером файловой системы для однозначного определения файла [4].

[8] Идентификатор родительского каталога – уникальное числовое значение, используемое драйвером файловой системы для установления соответствия между файлом и каталогом, в котором файл расположен [4].

[9] Имя файла – битовая строка, используемая драйвером файловой системы для представления файла пользователю [4].

[10] Символы, не являющиеся буквами, цифрами и пробелами будем относить к категории специальных при рассмотрении имен файлов.

- «Операция» – идентификаторы операций, принадлежащих R_G;
- «Имя», «Расширения», «Шаблоны имён», «Символы имени» – имена файлов, принадлежащих N_G;
- «USN» – номера записей;
- «Временная отметка» – временные отметки создания записей.

Говоря об оценке аномальности воздействия, следует отметить, что этот параметр непосредственно связан с процедурой экспертной оценки и определяется специалистом-аналитиком, подготавливающим шаблон воздействия на файл с целью последующей их (воздействий) идентификации в рамках расследования инцидента ИБ. Например, создавая шаблоны воздействий на файлы, в т.ч. при рассмотрении сценариев и примеров атаки типа «внедрение кода», специалист, используя признак $G_{anomaly}$, может пометить шаблоны как аномальные, то есть не являющиеся санкционированными в процессе штатного функционирования операционной системы и активности пользователя.

Признаки значимости I_{sign}, D_{sign}, R_{sign}, N_{sign} определяют необходимость использования значений из соответствующих множеств I_G, D_G, R_G, N_G при экспресс-анализе воздействий на файлы с использованием шаблонов. Каждый признак значимости может принимать значение 0 или 1, определяемое специалистом-аналитиком, подготавливающим шаблон, в зависимости от того, важны ли значения соответствующего множества при идентификации воздействия на файл с применением генерируемого шаблона. Стоит отметить, что поля, не выделенные как значимые, не будут учитываться в последующем применении шаблона воздействия для его идентификации в рамках экспресс-анализа событий. В свою очередь, чем точнее указаны значения полей шаблона воздействия, тем ниже вероятность появления ошибок 1 и 2 рода при проведении экспресс-анализа событий ИБ с применением шаблонов.

3.3. Применение базы данных шаблонов воздействий на файлы

Поиск и классификация воздействий на файлы с использованием шаблонов осуществляется на основе нахождения совпадений в записях журнала с данными шаблонов. Как отмечалось выше, воздействие на файл характеризуется значениями из множеств I_G, D_G, R_G, N_G, которые можно рассматривать как компоненты вектора G_f, характеризующего файл. Поскольку в контексте определённого воздействия те или иные компоненты могут быть значимыми или незначимыми и иметь различные значения из соответствующих множеств, то сравнение с шаблоном осуществляется пороговым способом по степени близости, рассчитываемой как взвешенное скалярное произведение компонент вектора G_f с соответствующими компонентами шаблона G.

Алгоритм поиска и классификации воздействий на файлы включает следующие операции (рис. 3):

1) открыть базу данных шаблонов; загрузить совокупность хранящихся в базе шаблонов и начать цикл по поиску соответствия шаблонов в наборе записей журнала;
2) загрузить из выбранного в цикле шаблона компоненты вектора G;
3) сформировать вектор-столбец максимальных весовых коэффициентов $W_{\max}$ (все компоненты вектора имеют ненулевое значение и по умолчанию имеют вес, равный 1). $W_{\max}$ описывает ситуацию, когда все компоненты вектора G, характеризующие воздействие, являются значимыми;
4) на основе признаков значимости I_{sign}, D_{sign}, R_{sign}, N_{sign} сформировать вектор-строку весовых коэффициентов W (по умолчанию вес равен 1). W описывает ситуацию, когда значимость компонентов вектора G, характеризующих файл, определяется соответствующими признаками;

5) умножением вектора-строки W на вектор-столбец $W_{\max}$ рассчитать пороговое значение $G_{threshold}$;

6) выбрать из журнала записи в соответствии со значимыми признаками шаблона G;

7) разделить выбранные записи на блоки по временным интервалам t для выделения воздействий из общего набора записей;

8) сравнить полученные блоки записей с текущим шаблоном G: для каждого признака текущего шаблона G найти вхождения (совпадения) значений признака в полях записей блоков и сформировать вектор-столбец вхождений $W_{similar}$;

9) рассчитать значение коэффициента сходства $G_{similar}$, умножив вектор-строку W на вектор-столбец $W_{similar}$;

10) сравнить $G_{similar}$ и $G_{threshold}$: если $G_{similar} \geq G_{threshold}$, то набор записей в блоке совпадает с шаблоном G;

11) принять решение об условной аномальности воздействия: если записи в блоке принадлежат временному интервалу инцидента ИБ, то классифицировать их как условно аномальные;

12) на основании признака аномальности $G_{anomaly}$ принять решение о классификации воздействия, совпавшего с шаблоном G, как аномального;

13) перейти к следующему шаблону.

Говоря об оценке вычислительной сложности предложенного алгоритма, следует учитывать, что наибольший вклад вносит процедура выборки записей журнала в соответствии со значимыми признаками шаблона G, вычислительная сложность которой за счёт использования двоичных деревьев поиска в индексах базы данных, хранящей записи загруженного журнала, составляет $O(n*\log_2 n)$, где n – количество записей журнала. В сравнении с другими популярными алгоритмами классификации, например, SVM ($O(n^2)$) или деревьям решений ($O(h+n*\log_2 n)$, где h – «глубина» дерева), предложенный алгоритм показывает лучшие или сопоставимые результаты, но устойчив к повышению вычислительной сложности из-за увеличения размерности пространства признаков (компонентов вектора G), а также позволяет менять дополнительные условия аномальности без необходимости переобучения классификатора.

4. Заключение

Существующие подходы к идентификации воздействий на файлы в рамках расследования инцидента ИБ опираются на анализ данных из множества массивов, таких как: журналы событий, последние открытые файлы, временные отметки файлов, объекты Jump List, объекты службы Prefetch, ветки реестра (UserAssist, MUICache, Persisted, BagMRU и др.), журналы стороннего программного обеспечения (например, Web-сервера), журналы средств защиты информации. Анализ указанных массивов данных позволяет определить порядок событий в рамках инцидента ИБ. В результате применения предложенного метода экспресс-анализа удалось сократить объём анализируемой специалистом информации. Вместо анализа совокупности данных о воздействиях на файлы, полученных из 8-12 массивов, упоминавшихся ранее, специалисту требуется проанализировать один массив данных – журнал изменений тома файловой системы NTFS $UsnJrnl.

Несмотря на то, что объем записей в журнале $UsnJrnl достигает 700–800 тысяч записей в зависимости от интенсивности осуществления файловых операций, применение подготовленной узкоспециализированной базы данных шаблонов для идентификации и классификации воздействий на файлы позволяет сконцентрировать внимание специалиста на нескольких десятках или сотнях записей, имеющих непосредственное отношение к расследуемому инциденту ИБ.

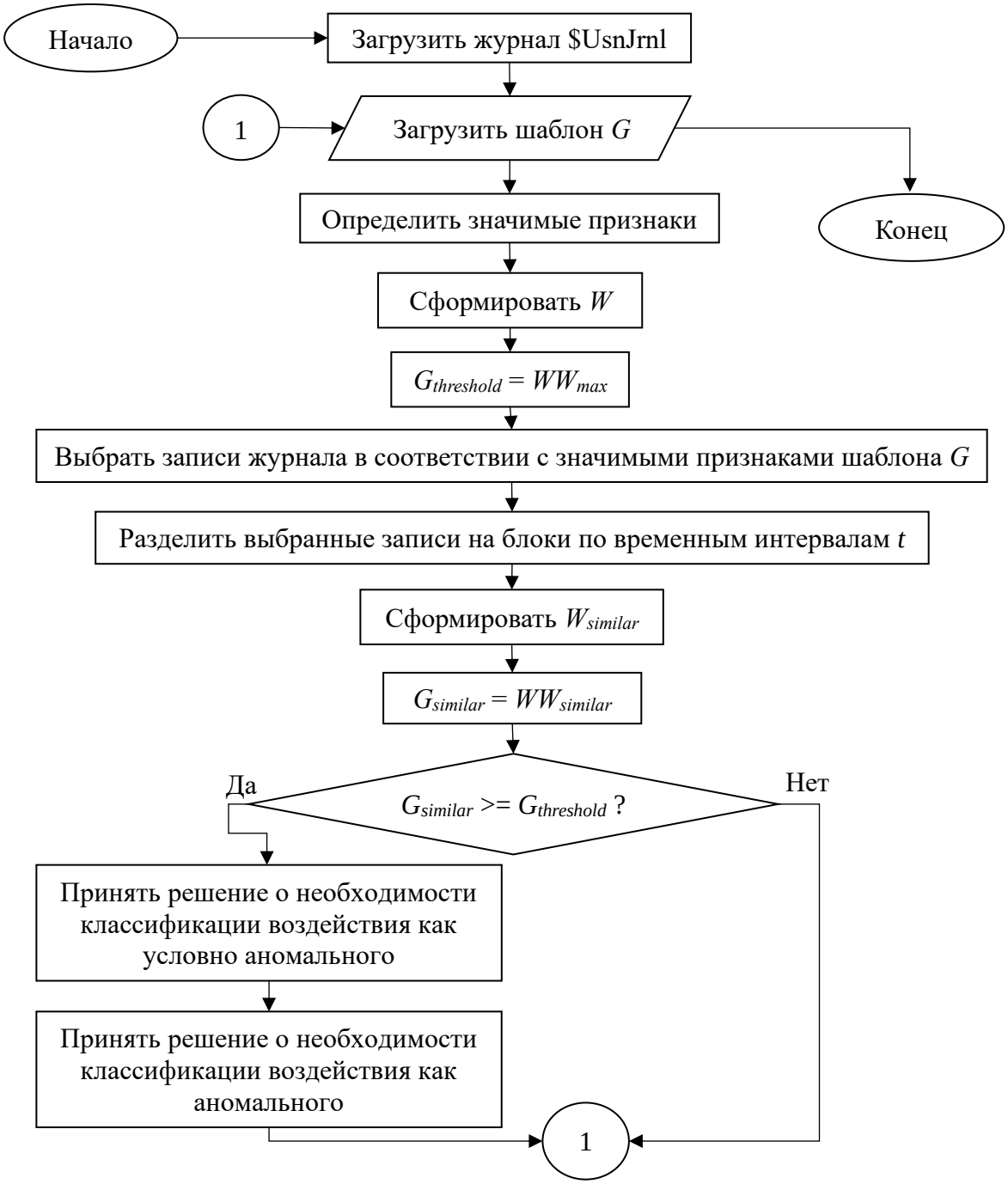

Рис. 3. Блок-схема алгоритма поиска и классификации воздействий на файлы с применением шаблонов

Литература

1. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М.: ФГУП «Стандартинформ», 2008. 30 с.
2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: ФГУП «Стандартинформ», 2006. 12 с.
3. ГОСТ 33707-2016 (ISO/IEC 2382:2015). Информационные технологии (ИТ). Словарь. М.: ФГУП «Стандартинформ», 2016. 548 с.
4. Стандарт Банка России СТО БР ИББС-1.3-2016 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств» [Электронный ресурс]. URL: http://garant.ru/products/ipo/prime/doc/71457690 (дата обращения: 06.06.2020).
5. *Гайдамакин Н. А., Гибилинда Р. В., Синадский Н. И.* Событийная модель процесса идентификации воздействий на файлы при расследовании инцидентов информационной безопасности, основанная на математическом аппарате сетей Петри // Вестник СибГУТИ. 2020. № 1. С. 73–88.
6. Jigsaw Ransomware Decrypted: Will delete your files until you pay the Ransom [Электронный ресурс]. URL: https://bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom (дата обращения: 06.06.2020).
7. *Dwyer J., Marius Truta T.* Finding Anomalies in Windows Event Logs Using Standard Deviation // 9th IEEE International on Collaborative Computing: Networking, Applications and Worksharing. 2013. P. 563–570.
8. *Бакланов В. В., Князева Н. С., Хорьков Д. А.* Анализ временных отметок файловой системы NTFS в операционной системе Microsoft Windows XP // Проблемы информационной безопасности. Компьютерные системы. 2012. № 4. С. 25–32.
9. UsnJrnl Parsing for File System History Project Report [Электронный ресурс]. URL: https://delaat.net/rp/2015-2016/p18/report.pdf (дата обращения: 06.06.2020).
10. USN_RECORD_V2 – Win32 apps [Электронный ресурс]. URL: https://docs.microsoft.com/en-us/windows/win32/api/winioctl/ns-winioctl-usn_record_v2 (дата обращения: 06.06.2020).

Статья поступила в редакцию 11.06.2020.

Гайдамакин Николай Александрович

д.т.н., профессор, профессор учебно-научного центра «Информационная безопасность» ИРИТ-РтФ УрФУ им. первого Президента России Б. Н. Ельцина (620002, Екатеринбург, ул. Мира, 19), e-mail: n.a.gaidamakin@urfu.ru.

Гибилинда Роман Владимирович

ассистент учебно-научного центра «Информационная безопасность» ИРИТ-РтФ УрФУ им. первого Президента России Б.Н. Ельцина, e-mail: r.v.gibilinda@urfu.ru.

Синадский Николай Игоревич

к.т.н., доцент, доцент учебно-научного центра «Информационная безопасность» ИРИТ-РтФ УрФУ им. первого Президента России Б.Н. Ельцина.

A method for rapid analysis of events related to impacts on files designed to investigate information security incidents

N. A. Gaidamakin, R. V. Gibilinda, N. I. Sinadsky

The article offers a method for rapid analysis of information security events based on the representation of an incident as a set of events consisting of impacts on files. The method involves using a database of identified impact templates, where initial data is the NTFS volume change log entries - $UsnJrnl. An algorithm for searching and classifying impacts on the files using templates is considered. The proposed method of rapid analysis allows you to determine the order of events within the framework of the incident under investigation, reducing the number of analyzed data arrays to one - $UsnJrnl log.

Keywords: information security incident investigation, information security event, file impact, file impact pattern.