004.056.53

РЕАЛИЗАЦИЯ ПРОГРАММЫ ДЛЯ ИССЛЕДОВАНИЯ ИНТЕРНЕТ-АКТИВНОСТИ ПОЛЬЗОВАТЕЛЯ

Чурсин Н.А.
студент группы БИТ-172
Омского государственного технического университета,
г. Омск
Данилова О.Т.
канд.физ.-мат. наук, доцент кафедры комплексной защиты информации
Омского государственного технического университета,
г. Омск

Аннотация. *В ходе решения поставленной задачи были затронуты вопросы, связанные с расследованием инцидентов информационной безопасности; построением поведенческой модели нарушителя на основе сетей Петри-Маркова; методом исследования интернет-активности пользователя. Исследован функционал программ для просмотров интернет запросов и скачиваемых файлов. В результате была разработана программа, позволяющая просматривать файлы баз данных различных браузеров, а также формировать отчет в форме, удобной форму для восприятия исследователем.*

Ключевые слова: *интернет-активность, история браузеров, компьютерно-техническая экспертиза, реализация программы.*

IMPLEMENTATION OF A PROGRAM FOR RESEARCH OF USER'S INTERNET ACTIVITY

Chursin N.A.
student of the Omsk State Technical University,
Omsk
Danilova O.T.
candidate of physical and mathematical Sciences, Associate Professor,
of the Omsk State Technical University,
Omsk

Annotation. *In the course of solving this problem, questions were raised about the methods of studying the user's Internet activity. The functionality of programs for viewing Internet requests and downloaded files is investigated. As a result, a program was developed that allows you to view database files of various browsers, which store all information about the user's Internet activity, and also converts the data into a more convenient form of perception by the expert.*

Keywords: *computer expertise; Internet-activity; browser history; computer and technical expertise; program implementation.*

Цели структурного подхода к менеджменту инцидентов информационной безопасности, изложенные в стандарте ГОСТ ИСО/МЭК 18044-2007, направлены для обеспечения следующих условий [1]:

1) обнаружение и эффективная обработка событий ИБ;
2) оценка и урегулирование событий ИБ наиболее подходящим и результативным способом;
3) минимизация соответствующими защитными мерами, являющимися частью процесса реагирования на инцидент, негативного воздействия инцидента ИБ;

4) разработка рекомендаций с целью повышения шансов предотвращения инцидентов ИБ в будущем, улучшения внедрения и использования защитных мер ИБ, улучшения общей системы менеджмента инцидентов ИБ.

Если инцидент ИБ определяется как «реальный», то, согласно плану реагирования, необходимо провести расследование, целью которого является немедленное подтверждение следующих пунктов:

1) что представляет собой инцидент ИБ, причины его возникновения, чем и кем был вызван;

2) определение потенциального объекта воздействия инцидента ИБ;

3) определение значительности инцидента;

4) подтверждение предумышленности атаки на ИС организации:

5) применение определенного способа обработки инцидента ИБ.

Расследование компьютерных инцидентов позволяет определить причину его возникновения, правильно обеспечить сбор и обработку доказательств и установить лицо, причастное к инциденту, что, в свою очередь, позволяет своевременно реагировать и минимизировать ущерб от подобных атак в дальнейшем [2].

В настоящей работе рассмотрены действия определенного типа внутренних нарушителей, совершающих свои действия умышленно, с целью получения выгоды. Поведенческая модель такого нарушителя построена на базе математического аппарата сетей Петри-Маркова [3]. Основными объектами модели являются: нарушитель (инсайдер), информационная система, а также конфиденциальные данные, на которые изначально нацелен инсайдер.

Поскольку нарушителем является непосредственно сотрудник, то следует пренебречь вероятностью преодоления возможных преград, предотвращающих доступ к конфиденциальным данным, и принять ее за единицу. Это объясняется тем, что инсайдер изначально имел все права на доступ к информации. Таким образом определим основные позиции поэтапного перехода нарушителя к достижению своей цели, которые будут являться элементами смоделированной сети, где позиции перехода – S_i и время между переходами – t_i. (рисунок 1).

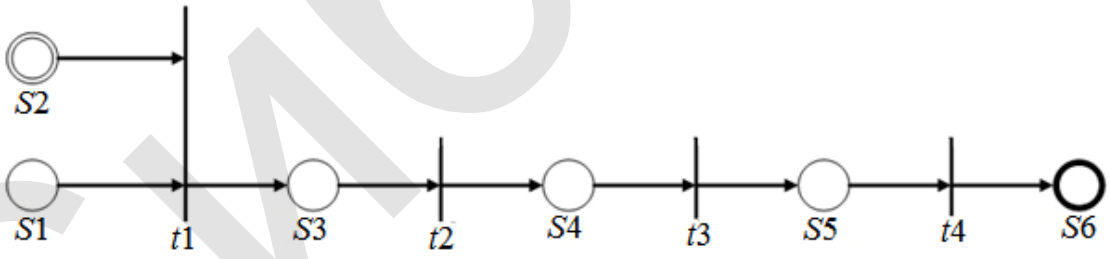

Рисунок 1 – Схематическая модель поведения инсайдера

Вход сотрудника в систему (*S*1) может быть реализован под закрепленными за ним пользовательскими данными, таким образом он получает доступ к объекту защиты. Далее потенциальный нарушитель приступает к поиску необходимого ему конфиденциального материала (*S*2) и, как следствие, обнаруживает защищаемую информацию (*S*3). Получив доступ к необходимой информации (*S*4), потенциальный нарушитель предпринимает определенный действия в отношении к ней (*S*5), в результате чего достигает задуманное им злонамеренное деяние (*S*6).

С момента входа в систему до поиска информации (*t*1), действия нарушителя фиксируются в журнале событий, который позволяет идентифицировать непосредственно злоумышленника, который намерен совершить противоправное действие, время его пребывания системе, а также события обращения к защищаемым данным. Дальнейшие действия до момента обнаружения конфиденциальной информации (*t*2 – *t3*), условно следует

определить, как последнюю активность пользователя, которая в большинстве своем сохраняется в реестре ОС. Сведения в реестре позволяют определить какими средствами руководствовался нарушитель (применялось ли специальное ВПО или внешний накопитель, программы редактирования документа или стирания следов, время использования и т.д.), чтобы осуществить кражу. На последнем этапе (*t*4) стоит задача передачи информации, и поскольку основным каналом является - сетевой, то в данном случае следует проанализировать файлы записи сетевой активности. Такими файлами могут являться логи сетевого ПО, например, файлы истории браузера, кэш-файлы, файлы cookie. В случае использования программ мгновенного обмена сообщениями, проанализировать файлы записи истории чата.

На основании данных действий, составляется модель расследования данного инцидента. Так на рисунке 2 показана контекстная диаграмма этапов анализа сетевой активности пользователя.

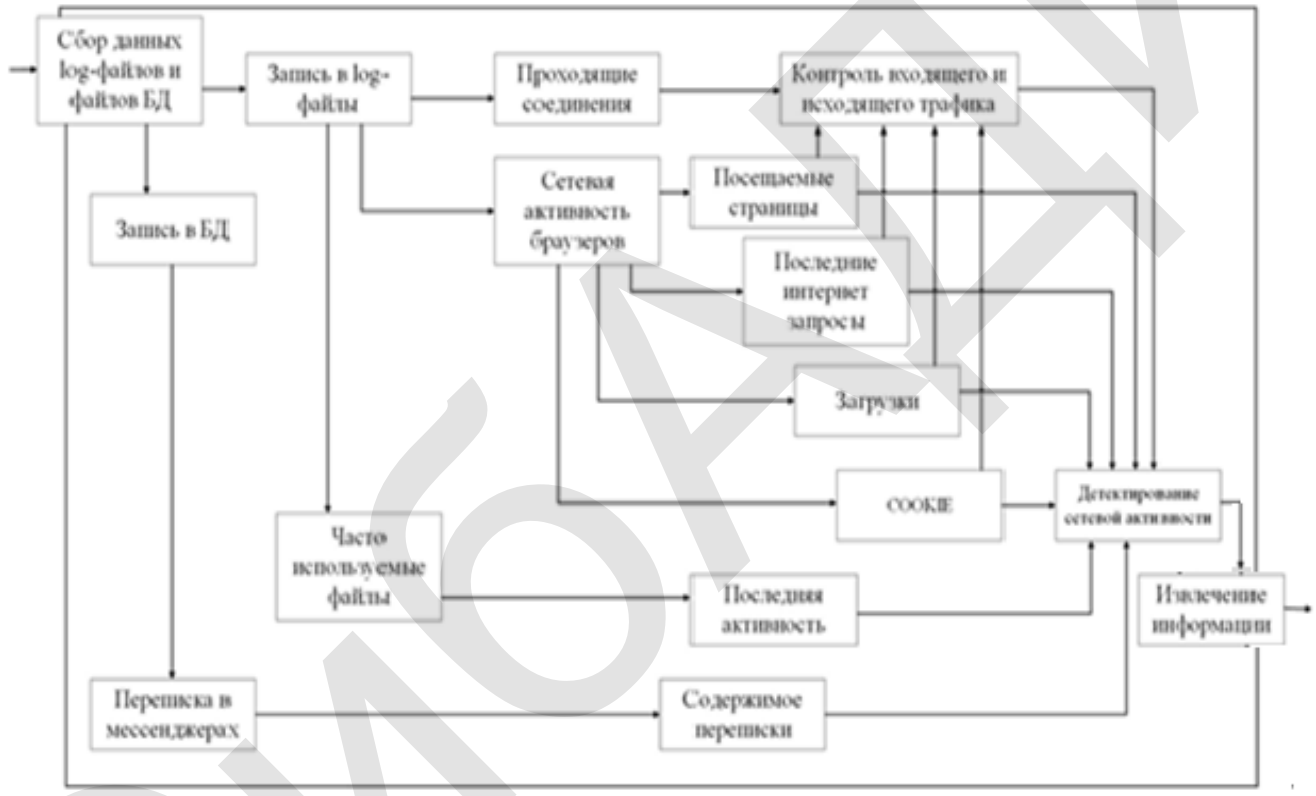

Рисунок 2 – Схема этапов анализа сетевой активности пользователя

При проведении расследований инцидентов, связанных с анализом действий пользователя, важным этапом является поиск информации, связанной с его интернет-активностью. Цифровые следы, оставляемые браузерами в процессе работы пользователя, составляют одну из составляющих при сборе доказательной базы [4]. Браузеры сохраняют историю сайтов в отдельный файл формата «log» или «dat». Для наиболее удобного просмотра и анализа содержимого истории необходимо применять специальное ПО. Файл находится в корне папки, в которой установлен браузер, в подпапке «History». История может записываться в один файл, а также в нескольких файлах, отдельно по каждому дню. Подобные файлы помечены в соответствии с датой и временем. Содержимое истории несет информации о сетевой активности, а именно, суммарное количество просмотренных веб-страниц, их URL-адреса, количество раз просмотра, время и дата просмотра, а также пользователя, который обращался к веб-ресурсу [5]. Каждый из веб-браузеров сохраняет историю в разных локациях, например, истории браузеров Chrome, Opera и Firefox расположены по следующему пути:

1) Chrome - %Drive%:\Users\{User_profile}\AppData\Local\Google\Chrome\UserData\Default;
2) Opera - %Drive%:\Users\{User_profile}\AppData\Roaming\Opera\Opera;
3) Firefox - %Driva%:\Users\{User_profile}\AppData\Roaming\Mozilla\Firefox\Profiles.

В ходе исполнения настоящего исследования разработана программа, позволяющая специалисту без какой-либо предварительной настройки, просматривать базы данных различных браузеров с поддержкой русского языка, а также со встроенным модулем, который преобразует данные по дате и времени в форму представления удобную для восприятия. Блок-схема программы представлена на рисунке 3.

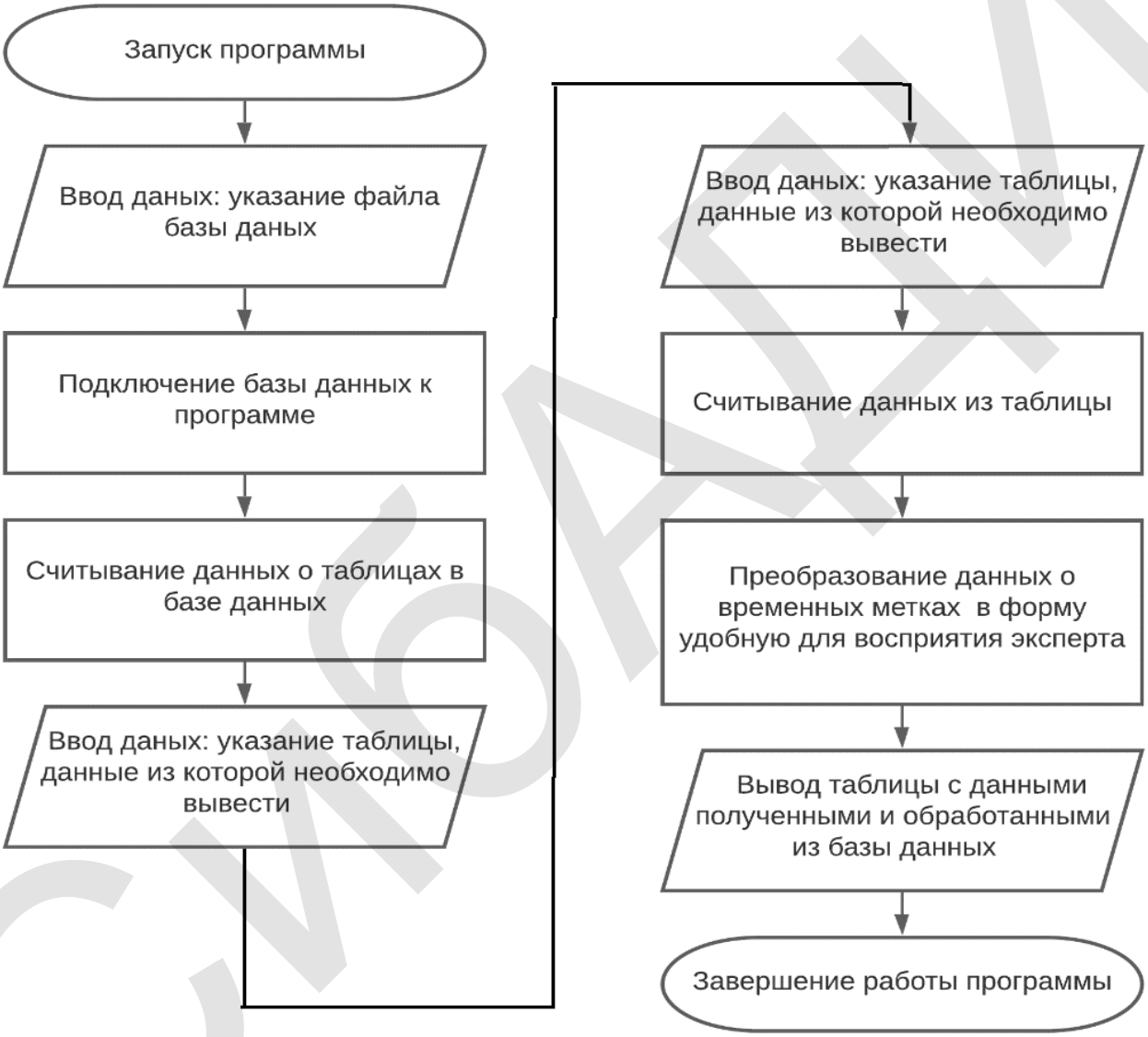

Рисунок 3 – Блок-схема программы

Так при обращении к соответствующей базе данных проводится считывание данных из таблицы. После операции считывания, анализируется информация, содержащая записи временных меток. В результате выполнения программы формируется отчет в удобной для чтения форме, фрагмент которого проиллюстрирован таблицей 1.

На основании представленной блок-схемы была разработана программа, в которой были реализованы все модули, указанные в блок-схеме.

Таблица 1 – Сведения из отчета, сформированного программой при анализе файлов истории браузера Chrome

d	url	title	visit_count	typed_count	last_visit_time	idden
	https://myip.ru/		1	0	19.10.2020 7:45:50	
	https://chrome.google.com/webstore/category/...	Интернет-магазин Chrome - Расширения	3	0	06.11.2020 16:39:07	
	https://chrome.google.com/webstore/search/.	Интернет-магазин Chrome - editthiscookie	1	0	13.10.2020 17:08:52	
	https://chrome.google.com/webstore/detail/.	EditThisCookie - Интернет-магазин Chrome	1	0	13.10.2020 17:09:11	
	https://chrome.google.com/webstore/detail/..	EditThisCookie - Интернет-магазин Chrome	1	0	13.10.2020 17:09:23	
	chrome-extension://fngmhnnpilhplaeedifhc…		1	0	13.10.2020 17:09:31	
	chrome-extension://fngmhnnpilhplaeedifhc…	Поддержать EditThisCookie	1	0	13.10.2020 17:09:31	
	https://www.google.com/search?q...	включить расширения в инкогнито - Поиск в Google	2	0	13.10.2020 17:13:13	
	https://www.google.com/search?q=kali+download...	kali download - Поиск в Google	2	0	19.10.2020 18:41:55	
0	https://www.kali.org/downloads/	Official Kali Linux Downloads	3	0	19.10.2020 18:43:06	

Полученные результаты позволяют сделать следующие выводы:

1. Для эффективной обработки событий информационной безопасности необходимо построение поведенческой модели потенциального нарушителя.

2. На основании поведенческой модели можно разработать детальный план расследования инцидента информационной безопасности, что позволит специалисту определиться с набором необходимого аналитического инструментария.

Так в настоящей работе было разработано программное обеспечение, позволяющее проводить анализ историй различных браузеров, а также формировать отчет в форме удобной для восприятия.

Библиографический список

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – М.: Стандартинформ, 2009. – 50 с

2. ГОСТ Р ИСО/МЭК 27001–2006. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. – Введ. 2006–12–27. – М.: Изд-во стандартов, 2008. – 31 с.

3. Марков, А.В. Применение матричного представление сетей Петри к различным системам / А.В. Марков. – Международная научная конференция «Математическое и компьютерное моделирование», 18-19 октября 2013 г. – Омск: Изд-во ОГУ, 2013. – С. 29–34.

4. Hutchins, E. M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains/ E.M. Hutchins, M.J. Cloppert, R.M. Amin //Leading Issues in Information Warfare & Security Research. – 2011. – Т. 1. – №. 1 – 80 с.

5. Расследование инцидентов ИБ: Как расследовать разглашение конфиденциальной информации в блогах и форумах. – URL: http://forensics.ru/investigation_blogs.html (дата обращения 16.09.2020).