МОДЕЛИРОВАНИЕ СИСТЕМ

УДК 004.056.53

РАЗРАБОТКА МОДЕЛИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМЫ КОНТРОЛЯ УТЕЧЕК ИЗОБРАЖЕНИЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ЗА СЧЕТ РАЦИОНАЛЬНОГО ПЕРЕРАСПРЕДЕЛЕНИЯ РЕСУРСОВ

© 2022 М. А. Бугорский, А. Б. Сизоненко

Краснодарское высшее военное училище (Краснодар, Россия)

Для реализации задач по повышению эффективности функционирования подсистемы контроля утечек изображений автоматизированной системы в защищенном исполнении (АСЗИ) привлекают операторов центра мониторинга информационной безопасности (SOC) для анализа изображений с их последующей классификацией и поиском конфиденциального содержимого, применяют методы машинного зрения системы предотвращения утечек информации (DLP-система) для поиска и контроля в информационном потоке изображений любого содержания, учитывая возможные изменения разрешения или расширения файла. Однако, существует необходимость рационального перераспределения ресурсов эргатической системы при обработке входящего потока изображений с целью избегания утечек изображений с конфиденциальной составляющей.

Ключевые слова: оператор, DLP-система, SOC-центр, эргатическая система, перераспределение ресурсов.

Стремление получить доступ к конфиденциальным данным со стороны организованной киберпреступности становится все более интенсивным, количество атак неуклонно увеличивается, цена утечки сильно возросла с начала специальной военной операции, и выявление внутренних злоумышленников стало еще более актуальной задачей для служб безопасности компаний по всему миру [1].

В настоящее время перед органами по защите информации стоит множество задач по обнаружению неочевидных угроз информационной безопасности, систематизированию данных и ликвидированию серых зон, выявлению путей распространения информации внутри компании, прогнозированию рисков информационной безопасности и оценке эффективности работы сотрудников. Иными словами, необходимо уметь предотвращать, а не только контролировать утечку информации.

Для реализации таких целей существует DLP-система InfoWatch Traffic Monitor. Она раскрывает перед операторами все вышеописанные возможности и полезна тем, что выявляет и блокирует утечки конфиденциальной информации любого формата, а также позволяет распознать мошеннические схемы, злой умысел и недобросовестных сотрудников [1].

Аналитический центр InfoWatch 15 августа 2022 года подготовил традиционный отчет по итогам исследования утечек информации за первое полугодие календарного года.

Так, по итогам первой половины 2022 г. в мире зарегистрирована 2101 утечка информации ограниченного доступа, что почти в два раза больше, чем за аналогичный период прошлого года. Количество утечек информации в России за аналогичный период составило 305 (рис. 1).

Бугорский Михаил Андреевич – Краснодарское высшее военное училище, адъюнкт, mr.bugorskey@mail.ru. Сизоненко Александр Борисович – Краснодарское высшее военное училище, начальник кафедры, доктор технических наук, доцент, Siz_al@mail.ru.

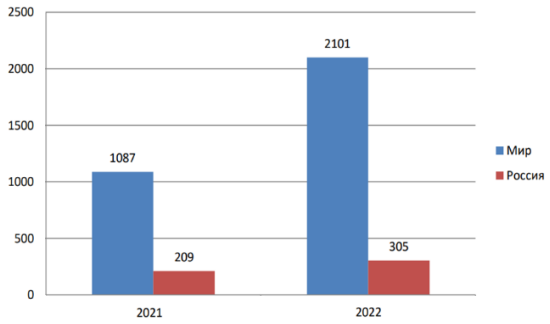

Рисунок 1. Анализ утечек информации за первые полугодия 2021 и 2022 гг.

На основании актуальности описанной проблемы и требований нормативно правовых актов в области защиты информации текущее исследование будет направлено на совершенствование предотвращения утечек изображений, содержащих информацию ограниченного распространения с помощью синтеза DLP-системы и SOC, а также с помощью рационального перераспределения ресурсов системы.

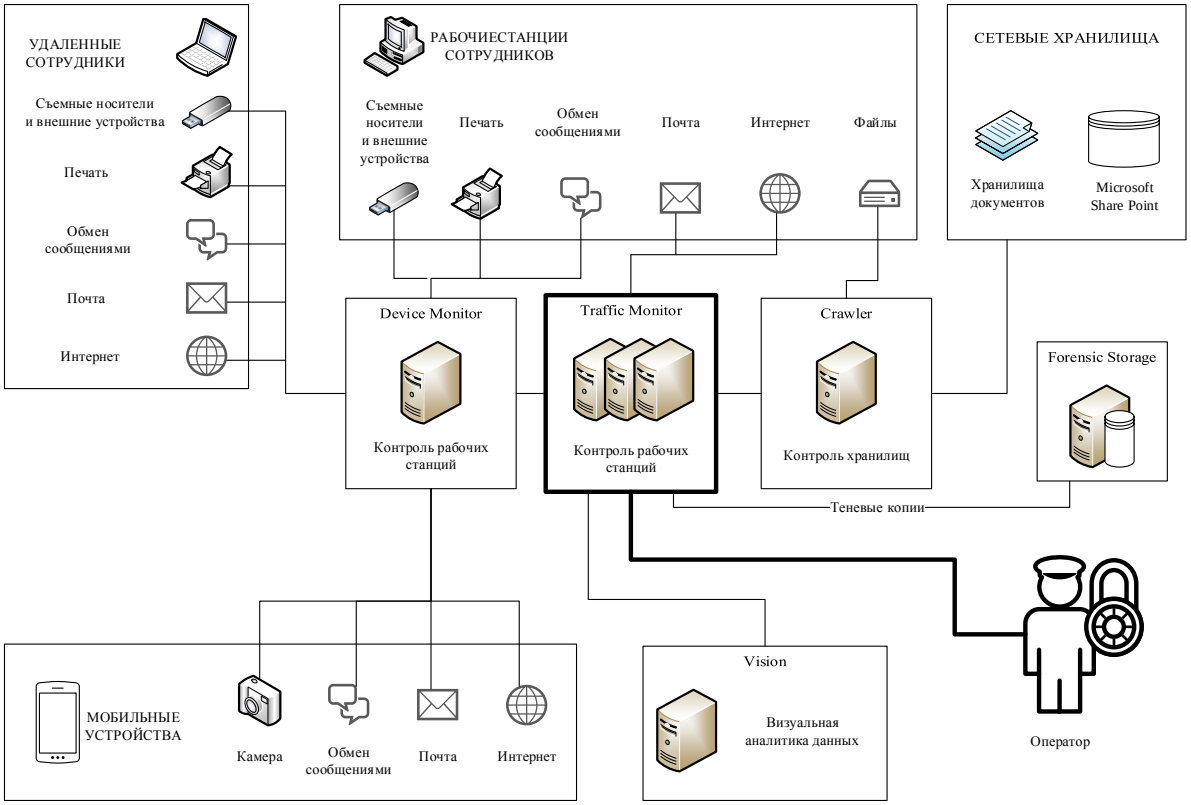

Рисунок 2. Функциональная модель DLP-системы InfoWatch

На рисунке 2 представлена область текущего исследования и выделена подсистема «Traffic Monitor – оператор» в качестве объекта исследования.

Подсистема выявляет сложные текстовые и графические объекты даже в случае, если нарушитель сумел значительно видоизменить их и ухитрился замаскировать свои действия. Благодаря многомерному анализу содержания, InfoWatch Traffic Monitor понимает, о какой информации идет речь. Это облегчает оператору работу с ошибками первого рода (ложноположительными срабатываниями).

В рамках предложенного синтеза получим эргатическую систему «человек — информация» (ЭС), образующуюся в процессе осуществления операторами SOC практической деятельности при проведении интеллектуализированной человекоинформационной связи с подсистемой Traffic Monitor DLP-системы InfoWatch [3].

Так как в работе ЭС существуют такие понятия как производительность вычислительных устройств, которые могут быть

использованы DLP-системой, объем памяти, выделяемый DLP-системе и человеческий ресурс, определяемый как количество операторов SOC, которые могут быть задействованы для анализа изображений, поступающих от DLP-системы, то задачей ЭС является определение оптимальных параметров АСЗИ таких как результативность, ресурсоемкость и оперативность в работе с входящим потоком изображений.

Применим методы аналитического моделирования для формализованного обоснования рационального перераспределения ресурсов.

Введем обозначения:

E – показатель эффективности:

$$E = \frac{Res}{Rez} \quad (1)$$

Rez – показатель результативности:

$$Rez = \frac{Rez_{\text{факт}}}{Rez_{\text{тр}}} \cdot 100\% \quad (2)$$

Res – показателей ресурсоемкости:

$$Res = \{Res_{PU}, Res_{M}, Res_{Stf}\} \quad (3)$$

T – показатель оперативности.

PU – суммарный показатель производительности вычислительных устройств, которые могут быть использованы DLP-системой;

M – объем памяти, выделяемый DLP-системе;

Stf – человеческий ресурс, определяемый как количество операторов SOC, которые могут быть задействованы для анализа информации, поступающей от DLP-системы.

Из формулы (1) получаем, что повышение эффективности системы зависит от отношения производительности вычислительных устройств, объема выделяемой системе памяти и количества операторов SOC к отношению фактической и требуемой результативности.

Получим ограничения:

$$\begin{cases} Rez \le Rez_{\text{тр}} \\ Res \le Res_{\text{доп}} \\ T - const \end{cases} \quad (4)$$

Получим допущения:

$$\begin{cases} PU \le PU_{\text{доп}} \\ \text{M} \le \text{M}_{\text{доп}} \\ Stf \le Stf_{\text{доп}} \end{cases} \quad (5)$$

Таким образом, стремление повысить эффективность системы приводит к необходимости построения ее модели. В связи с необходимостью выражения всех исследуемых свойств процессов в форме количественных характеристик и на основании вышеописанной формализации, была произведена декомпозиция ЭС, установлены взаимосвязи элементов [2], а впоследствии создана модель функционирования ЭС в среде моделирования AnyLogic 8 Personal Learning Edition.

Данная модель позволяет в режиме реального времени изменять интенсивность входящего потока изображений, мощность DLP-системы для изменения качества классификации изображений, время на обработку изображения оператором SOC для учета человеческих факторов и количество операторов SOC. Также модель позволяет отслеживать общее количество поступивших в систему изображений, верно классифицированных системой, и изображений, направленных на обработку к операторам SOC (рис. 3).

Анализ информационных потоков и поведенческая аналитика способны не только предотвращать инциденты, связанные с человеческим фактором, целенаправленными атаками и утечкой данный, но и предсказывать вероятность возникновения рисков и находить пути повышения эффективности.

Таким образом можно формулировать задачи поиска оптимальных параметров подсистемы системы предотвращения утечек информации такие как поиск минимального количества операторов SOC, формализовывать поставленные задачи и с помощью полученной модели получать количественную оценку выдвинутых теорий.

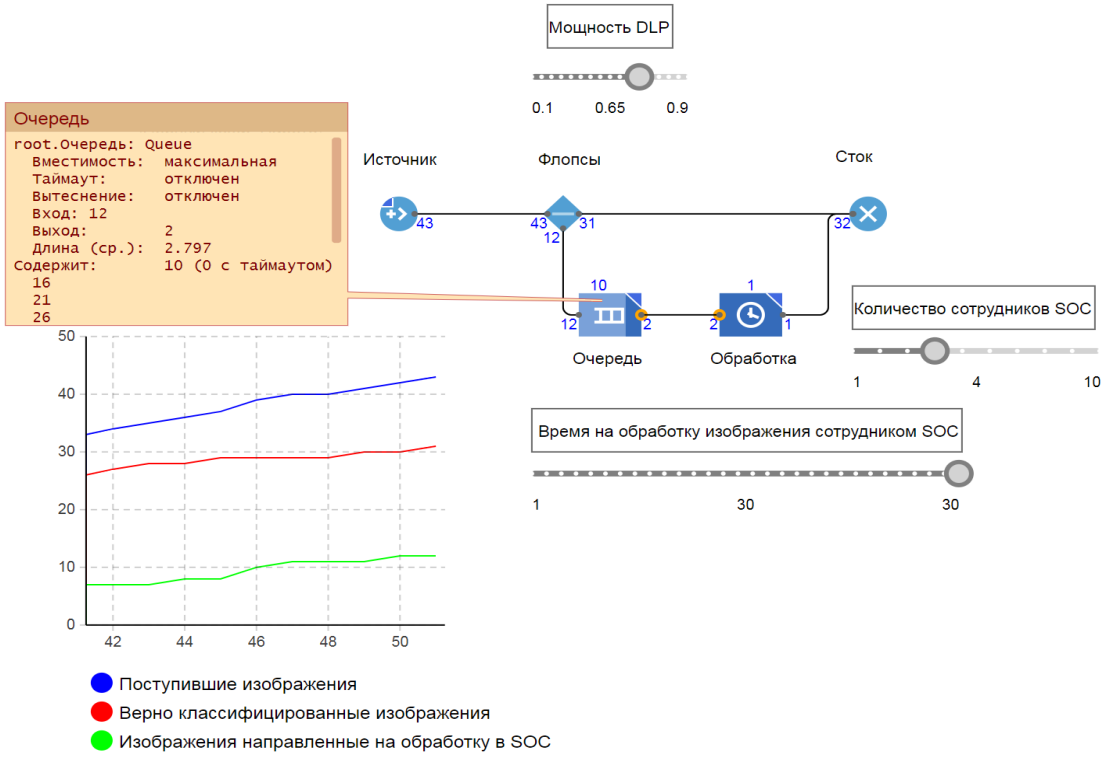

Рисунок 3. Модель функционирования ЭС

СПИСОК ИСТОЧНИКОВ

1. Аналитика InfoWatch. Международные новости утечек информации, ежегодные аналитические отчеты и статистика по инцидентам за прошедшие годы. [Электронный ресурс]. – Доступно по: https://www.infowatch.ru/analytics/analitika/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda (дата обращения: 24.11.2022).

2. Петров А. В. Моделирование процессов и систем: Учебное пособие / А. В. Петров. – СПб.: Издательство «Лань», 2015. – 288 с.

3. ГОСТ 43.4.1 – 2011. Информационное обеспечение техники и операторской деятельности система «человек – информация»: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 13 декабря 2011 г. № 1243-ст – URL: https://docs.cntd.ru/document/1200094359 (дата обращения: 24.11.2022). – Текст: электронный.

PERFORMANCE IMPROVEMENT MODEL SUBSYSTEMS OF IMAGE LEAKAGE CONTROL OF AUTOMATED SYSTEM IN PROTECTED PERFORMANCE DUE TO RATIONAL REDISTRIBUTION OF RESOURCES

© 2022 M. A. Bugorsky, A. B. Sizonenko

Krasnodar Higher Military School (Krasnodar, Russia)

To implement the tasks of improving the efficiency of the image leak control subsystem of an automated secure system (APIS), operators of the information security monitoring center (SOC) are involved in image analysis with their subsequent classification and search for confidential content, and machine vision methods of the prevention system are used. information leaks (DLP-system) for searching and controlling images of any content in the information stream, taking into account possible changes in the resolution or extension of the file. However, there is a need to rationally redistribute the resources of the ergatic system when processing the incoming image stream in order to avoid leakage of images with a confidential component.

Keywords: operator, DLP system, SOC center, ergatic system, redistribution of resources.