Автоматизация и моделирование в проектировании и управлении. 2022. № 3 (17). С. 4-9.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2022. № 3 (17). P. 4-9.

Автоматизация и управление технологическими процессами и производствами, системы автоматизации проектирования

Научная статья
Статья в открытом доступе
УДК 004.056.53
doi:10.30987/2658-6436-2022-3-4-9

АНАЛИЗ ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМЫ КОНТРОЛЯ УТЕЧЕК ИНФОРМАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Михаил Андреевич Бугорский
Краснодарское высшее военное училище, г. Краснодар, Россия
bugorskey@mail.ru

Аннотация. *Целью исследования данной статьи является повышение эффективности функционирования подсистемы контроля утечек информации автоматизированной системы в защищенном исполнении за счет рационального перераспределения ресурсов. Частной научной задачей является анализ функционирования подсистемы контроля утечек информации автоматизированной системы в защищенном исполнении. В качестве методов исследования был выбран анализ архитектур системы предотвращения утечек информации и центра мониторинга информационной безопасности с выделением их недостатков. Впоследствии, представлен синтез архитектур системы предотвращения утечек информации и центра мониторинга информационной безопасности, а также описана формальная постановка задачи. Новизна исследования состоит в разработке модели и методики оценки эффективности функционирования подсистемы контроля утечек информации автоматизированной системы в защищенном исполнении. В результате анализа функционирования подсистемы контроля утечек информации автоматизированной системы в защищенном исполнении был выявлен ряд недостатков и представлен способ их решения. Таким образом, для решения поставленной задачи введены параметры, определение оптимальности которых минимизирует утечку информации в автоматизированной системы в защищенном исполнении.*

Ключевые слова: автоматизированная система в защищенном исполнении, контроль утечек информации, оценка эффективности, DLP-система, SOC

Для цитирования: Бугорский М.А. Анализ функционирования подсистемы контроля утечек информации автоматизированной системы в защищенном исполнении // Автоматизация и моделирование в проектировании и управлении. 2022. №3 (17). С. 4-9. doi: 10.30987/2658-6436-2022-3-4-9.

Original article
Open Access Article

ANALYSING INFORMATION LEAK CONTROL SUBSYSTEM OF A PROTECTED AUTOMATED SYSTEM

Mikhail A. Bugorsky
Krasnodar Higher Military School, Krasnodar, Russia
bugorskey@mail.ru

Abstract. *The aim of the study is to increase the efficiency of the information leak control subsystem of a protected automated system based on the rational redistribution of resources. The article is devoted to solving a specific scientific problem to analyse the information leak control subsystem of a protected automated system. The research method is analysing the architectures of the information leak prevention system and the information security monitoring centre, highlighting the architecture shortcomings. Subsequently, the architecture synthesis of the information leak prevention system and the information security monitoring centre is presented, also the formal statement of the problem is described. The novelty of this study lies in developing a model and methodology for evaluating the efficiency of the information leak control subsystem of a protected automated system. As an analysis result of operating the information leak control subsystem of a protected automated system, a number of shortcomings are identified and a method for solving them is presented. Thus, to solve the problem, parameters are introduced and determining their optimality minimises information leakage of a protected automated system.*

Keywords: protected automated system, information leak control, performance evaluation, DLP system, SOC
For citation: Bugorsky M.A. Analysin information leak control subsystem of a protected automated system. Automation and modeling in design and management, 2022, no. 3 (17). pp. 4-9. doi: 10.30987/2658-6436-2022-3-4-9.

Введение

В соответствии с данными InfoWatch ежегодно растет количество утечек информации. Аналитический центр InfoWatch, провел глобальное исследование инцидентов внутренней информационной безопасности. Целью исследования было выявить все утечки конфиденциальной информации за последние четыре года проанализировать их характер (рис. 1) [1].

Рис. 1. Распределение утечек по типам данных: Мир, 2018-2021 гг
Fig. 1. Distribution of leaks by data type: World, 2018-2021

Исходя из анализа представленных в исследовании данных, можно предположить, что системе не хватает дополнительного модуля, который будет состоять из специалистов, отвечающих за оперативный мониторинг и анализ информационной среды.

Актуальность исследования обусловлена требованиями нормативно-правовых актов и существующим положением дел [1 – 8] и заключается в том, что существует необходимость в:

– обработке больших объемов данных;
– развитии искусственного интеллекта;
– подготовке квалифицированных кадров в сфере информационных и коммуникационных технологий.

Материалы

Data Leakage Prevention (DLP) – системы предотвращения утечек информации. Подобного рода системы создают защищенный цифровой периметр вокруг организации, анализируя всю исходящую, а в ряде случаев и входящую информацию (рис. 2).

Недостатки системы DLP:

1) возможна остановка процессов организации, так как у активных DLP-систем есть полномочия своим решением блокировать или останавливать процессы в случае инцидента;

2) существует риск случайных утечек информации, иными словами, вероятность ложно-отрицательных срабатываний системы (пропуск цели) или ошибки II-рода;

3) необходимость выделения специалистов для регулярного и непрерывного мониторинга событий;

4) требуются большие ресурсы для хранения архивных журналов событий;

5) наличие внутренних субъективных угроз. Руководители организации и/или администраторы безопасности системы могут искажать результаты работы DLP-системы.

Одним из решений всех вышеупомянутых недостатков является центр мониторинга информационной безопасности (Security Operations Center – далее SOC) – это структурное подразделение организации, отвечающее за оперативный мониторинг IT-среды и предотвращение киберинцидентов. Специалисты SOC собирают и анализируют данные с различных объектов инфраструктуры организации и при обнаружении подозрительной активности принимают меры для предотвращения атаки (рис. 3)

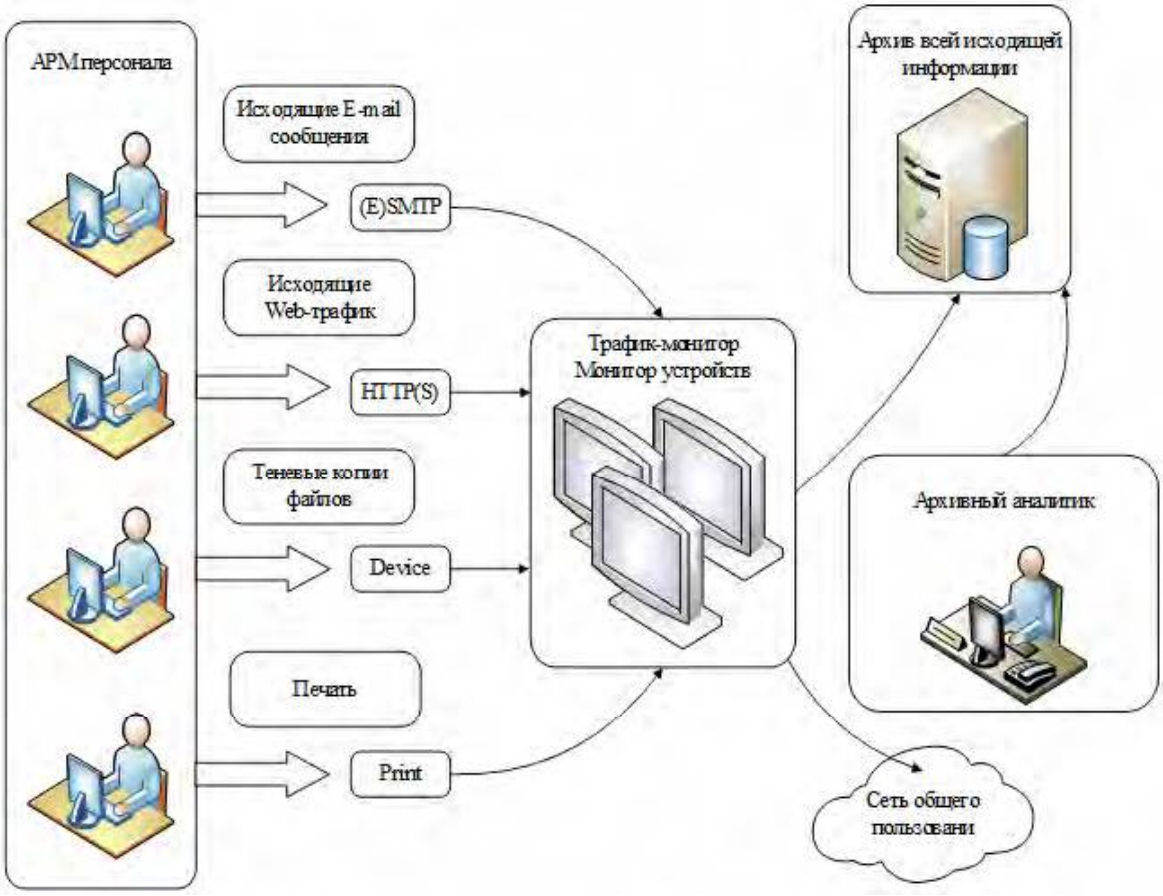

Рис. 2. Архитектура DLP-системы
Fig. 2. DLP system architecture

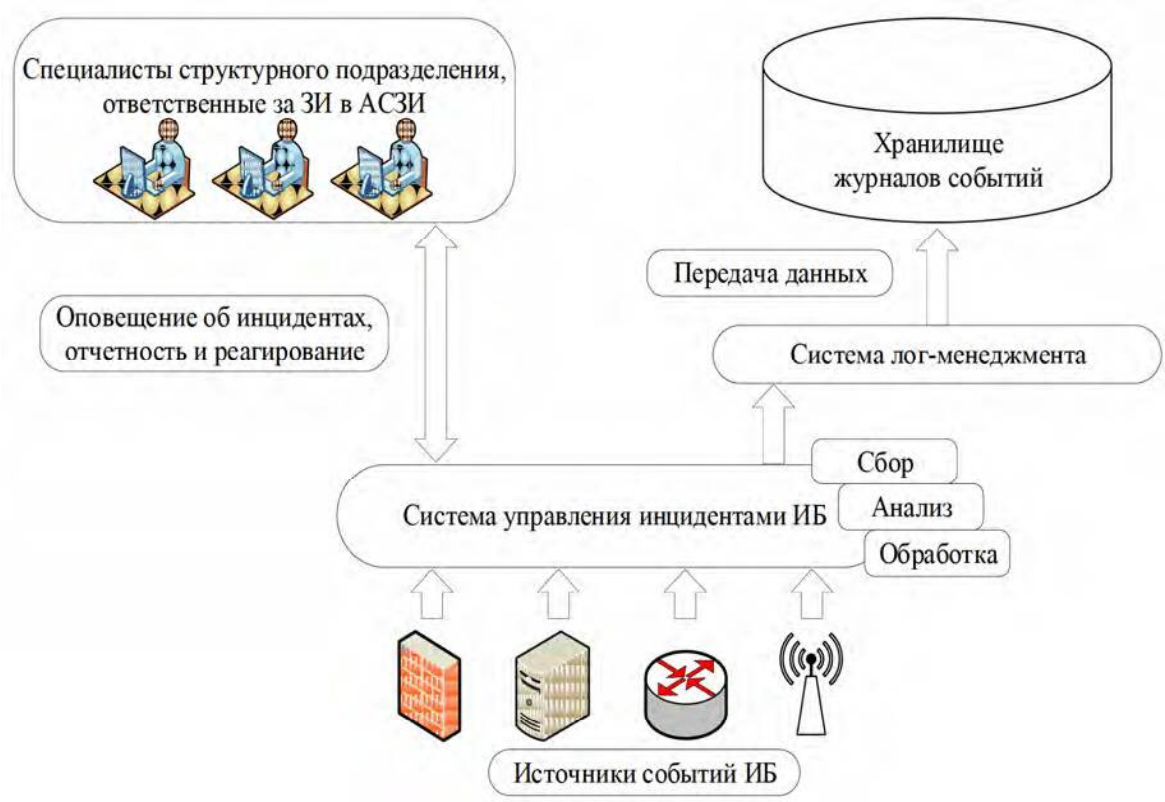

Рис. 3. Архитектура SOC
Fig. 3. SOC architecture

Недостатки SOC:

1) нехватка в составе SOC квалифицированного персонала;

2) приоритет распределения бюджета в сторону внедрений технических решений, что приводит к недостаточному количеству специалистов;

3) отсутствие механизма обнаружения целенаправленных атак;

4) неправильный выбор расписания работы сотрудников;

5) не существует эффективной автоматизации.

Отметим, что такую функцию DLP-системы, как обнаружение и блокировка утечек выполняет подсистема контроля утечек информации, улучшая показатели которой мы обеспечим выполнение функции обнаружения и блокировки.

Результаты

В ходе проведенного анализа был выявлен ряд противоречий между необходимостью комплектования специалистами в области информационной безопасности для регулярного и непрерывного мониторинга событий, повышения количества выделяемых аппаратных ресурсов для хранения больших объемов данных и отсутствием моделей и алгоритмов классификации изображений в подсистеме контроля утечек автоматизированной системы в защищенном исполнении, а также отсутствием моделей и алгоритмов повышения эффективности классификации информации подсистемы контроля утечек в автоматизированной системе в защищенном исполнении за счет рационального перераспределения ресурсов.

Таким образом, был предложен синтез DLP-системы и с полным или частичным привлечением сотрудников SOC (рис. 4).

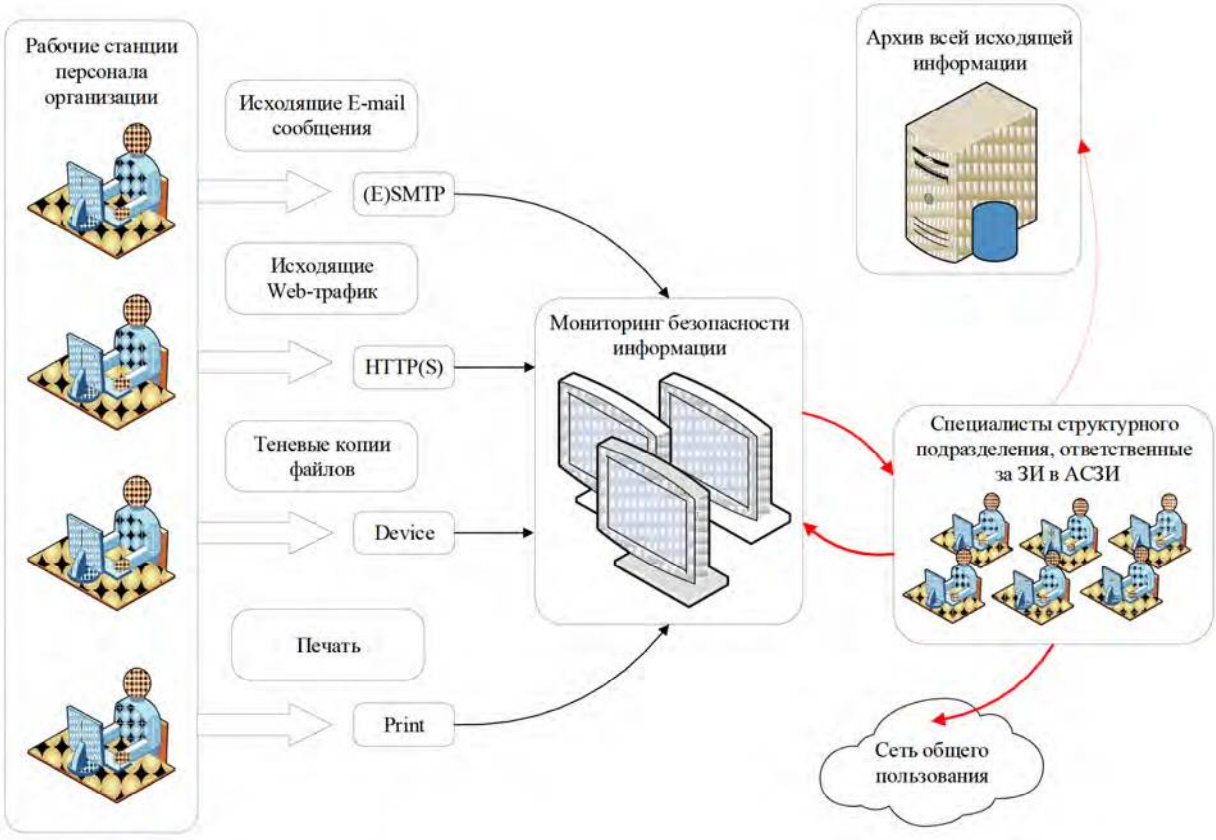

Рис. 4. Архитектура взаимодействия SOC с DLP-системой

Fig. 4. Architecture of interaction between SOC and DLP system

В ходе исследования требуется создать такую модель функционирования подсистемы, чтобы ее обобщенный показатель эффективности E стремился к максимуму, за счет повышения показателя результативности *Rez* и уменьшения множества показателей ресурсоемкости *Res*.

$$E = f(Rez, Res, T) \rightarrow max, \quad (1)$$

$$Res = f(PU, M, P) \rightarrow min. \quad (2)$$

Помимо этого, необходимо выполнение таких условий, чтобы полученный показатель результативности был больше требуемого за счет выделения допустимого количества ресурсов или их меньшего количества, не учитывая показатель оперативности T.

$$\begin{cases} Rez \geq Rez^{\text{тр}} \\ Res \leq Res^{\text{доп}}. \\ T - const \end{cases} \quad (3)$$

В свою очередь, множество показателей ресурсоемкости состоит из суммарного показателя производительности вычислительных устройств, которые могут быть использованы DLP-системой PU, объема памяти, выделяемого DLP-системе M и человеческого ресурса P, определяемого как количество человек из дежурной смены SOC, которые могут быть задействованы для анализа информации, поступающей от DLP-системы.

Уменьшая любой из этих показателей ниже допустимых значений, мы добьемся повышения значения обобщенного показателя эффективности.

$$\begin{cases} PU \leq PU^{\text{доп}} \\ M \leq M^{\text{доп}} \\ P \leq P^{\text{доп}} \end{cases} \quad (4)$$

Оптимальный показатель результативности предлагается оценивать с помощью AUC-ROC – площадь (Area Under Curve) под кривой ошибок (Receiver Operating Characteristic curve).

Заключение

Анализируя тенденции утечек информации в информационных системах, требования к автоматизированным системам в защищенном исполнении и возможности DPL-систем, можно сделать вывод, что синтез DLP-систем и SOC является актуальным способом в целях повышения эффективности контроля утечек информации.

Список источников:

1. Аналитика InfoWatch. Международные новости утечек информации, ежегодные аналитические отчеты и статистика по инцидентам за прошедшие годы. [Электронный ресурс] – URL: https://www.infowatch.ru/analytics/analitika/v-2021-stalo-bolshe-umyshlennykh-utechek (дата обращения: 17.06.2022)
2. Баранов А.Н., Баранова Е.М., Борзенкова С.Ю. Система защиты автоматизированной системы распределенной обработки информации // Известия Тульского государственного университета. Технические науки. 2019. № 12. С. 386-393.
3. Валиев И.А., Шустов К.В., Митрофанова Л.Х. Комплексная система защиты информации в организации // Производственный менеджмент: теория, методология, практика. 2016. № 8. С. 37-44.
4. Митрофанова Я.С. Создание типовой комплексной системы защиты информации на основе процессного моделирования // Информационные системы и технологии: управление и безопасность. 2016. № 4. С. 105-122.
5. Просис К., Мандиа К. Расследование компьютерных преступлений. – М.: Лори, 2017. С. 476.
6. Рогозин Е.А., Никулина Е.Ю., Попов А.Д. Основные этапы и задачи разработки систем защиты информации ОВД в автоматизированных системах // Вестник Воронежского института ФСИН России. 2016. № 4. С. 94-99.

References:

1. Analytics InfoWatch. International News of Information Leaks, Annual Analytical Reports and Statistics on Incidents over the Past Years [Internet] [cited 2022 Jun 17]. Available from: https://www.infowatch.ru/analytics/analitika/v-2021-stalo-bolshe-umyshlennykh-utechek.
2. Baranov A.N., Baranova E.M., Borzenkova S.Yu. Protection System for an Automated System for Distributed Information Processing. Izvestiya TulGU. Technical Sciences. 2019;12:386-393.
3. Valiev I.A., Shustov K.V., Mitrofanova L.Kh. Integrated Information Security System in an Organization. Production Management: Theory, Methodology, Practice. 2016;8:37-44.
4. Mitrofanova Ya.S. Creating a Typical Integrated Information Security System Based on Process Modelling. Information Systems and Technologies: Management and Safety. 2016;4:105-122.
5. Prosis K., Mandia K. Investigating Computer Crimes. Moscow: Lori; 2017.
6. Rogozin E.A., Nikulina E.Yu., Popov A.D. The Main Stages and Tasks of Developing Information Security Systems for Internal Affairs Bodies in Automated Systems. Vestnik of Voronezh Institute of the Russian Federal Penitentiary Service. 2016;4:94-99.

7. Селифанов В.В., Степанова С.В., Стрихарь Н.А., Звягинцева П.А., Чернов Д.В. Особенности выбора средств защиты информации в государственных информационных системах // Известия Тульского государственного университета. Технические науки. 2018. № 10. С. 18-21.
8. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. – М.: НИУ Высшая школа экономики, 2011. 574 с.

7. Selifanov V.V., Stepanova S.V., Strihar N.A., Zvyagintseva P.A., Chernov D.V. Features of the Choice of Means of Information Protection in State InformationSystems. Izvestiya TulGU. Technical Sciences. 2018;10:18-21.

8. Serdyuk V.A. Organization and Technology of Information Protection: Detecting and Preventing Information Attacks in Enterprise Automated Systems. Moscow: NRU Higher School of Economics; 2011.

Информация об авторах

Бугорский Михаил Андреевич
адъюнкт очной штатной адъюнктуры Краснодарского высшего военного училища.

Information about authors:

Bugorsky Mikhail Andreevich
adjunct of the full-time postgraduate studies in Krasnodar Higher Military School.

Статья поступила в редакцию 26.07.2022; одобрена после рецензирования 05.09.2022; принята к публикации 09.09.2022.

The article was submitted 26.07.2022; approved after reviewing 05.09.2022; accepted for publication 09.09.2022.

Рецензент – Рытов М.Ю., кандидат технических наук, доцент, Брянский государственный технический университет.

Reviewer – Rytov M.Yu., Candidate of Technical Sciences, Associate Professor, Bryansk State Technical University.