УДК 004.056

АНАЛИЗ ПРОГРАММНЫХ СРЕДСТВ ДЛЯ АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Фильченков П.А.

магистрант кафедры защиты информации гр.367241

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Бойправ О.В. – кандидат технических наук, доцент, доцент кафедры ЗИ

Аннотация. В материалах доклада приведены результаты анализа наиболее распространенных и хорошо зарекомендовавших себя на практике программных средств для аудита безопасности информационных систем.

Ключевые слова: аудит безопасности, информационная система, программное средство, риски информационной безопасности, угроза безопасности.

Введение. В настоящее время информационные системы используются в деятельности предприятий всех отраслей экономики. Они необходимы для хранения, обработки и передачи информации. Это обстоятельство обуславливает актуальность реализации мер по защите информационных систем. В целях оценки эффективности реализации этих мер, а также их проверки на соответствие требованиям технических нормативных и правовых актов необходимо периодически проводить аудит информационной безопасности в целом и аудит безопасности информационных систем в частности. Под аудитом информационной безопасности понимают системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности предприятия/организации в соответствии с определенными критериями и показателями безопасности [1].

Проведение аудита информационной безопасности состоит из следующих этапов:

– инициирование процедуры аудита,

– сбор информации, необходимой для проведения аудита,

– анализ данных аудита,

– формирование и составление рекомендаций,
– подготовка аудиторского отчета.

При проведении аудита информационной безопасности рассматриваются следующие виды угроз безопасности: организационные, эксплуатационные, программно-технические, а также прочие аспекты обеспечения информационной безопасности, которые необходимо учесть в ходе проведения аудита, для определения их приоритетов [2]. Для увеличения эффективности процесса аудита безопасности информационных систем как одного из направлений аудита информационной безопасности часто используются специальные программные средства, т. к. с их применением аудитору легче оценивать меры по защите информации на предмет их соответствия требованиям, определять области, реализуемые в рамках которых мероприятия необходимо совершенствовать, обеспечивать единообразие реализуемых процедур [3]. К настоящему времени разработано большое количество программных средств, рекомендуемых для использования в ходе проведения аудита безопасности информационных систем. Каждое из таких программных средств характеризуется определенным набором функциональных возможностей, которые определяют способы их применения. В настоящей работе представлены результаты анализа функциональных возможностей

Основная часть.

В настоящее время наиболее часто используемыми программными средствами для аудита безопасности информационных систем являются *Efros Defence Operations, Alertix, Ankey SIEM NG, Kaspersky Unified Monitoring and Analysis Platform (KUMA), KOMRAD Enterprise SIEM, MaxPatrol SIEM, R-Vision, RuSIEM*. В таблице 1 приведено краткое описание и особенности этих программных продуктов для проведения аудита безопасности информационных систем.

Таблица 1 – Программные средства для аудита безопасности информационных систем

№	Наименование программного средства	Краткое описание программного средства	Особенности программного средства
1	*Efros Defence Operations*	Многофункциональный комплекс по защите ИТ-инфраструктуры (сетевых и оконечных устройств, компонентов сред виртуализации), а также прикладного ПО: *SCADA, RPA*, СУБД. 1 ноября 2023 получил награду *CNews Awards* в номинации «Защита ИТ-инфраструктуры: платформа года».	Контроль конфигураций и топологии сети Контроль целостности и проверки соответствия хостов и конечных точек Оптимизация и настройка межсетевых экранов (далее – МЭ) Анализ уязвимостей и построение векторов атак Сбор и отображение статистики по потокам данных в сети Централизованная сетевая идентификация администраторов и управление доступом на сетевых устройствах, у которых на клиентском уровне поддерживаются протоколы *TACACS+* и (или) *RADIUS* Автоматизация управления МЭ

№	Наименование программного средства	Краткое описание программного средства	Особенности программного средства
2	*Alertix*	Система представлена на рынке с 2019 г. В функциональные возможности системы входит интеграция с НКЦКИ для оперативного оповещения об инцидентах на объектах КИИ. Сбор событий реализован агентским и неагентским способами.	Блокнот аналитика; Организация взаимодействия с НКЦКИ; управление конфигурацией *Sysmon* и *Beats* Бессрочные лицензии Гибкое управление глубиной хранения и архивации событий от источников
3	*Ankey SIEM NG*	Основными компонентами программного комплекса являются серверы сбора, обработки и хранения событий, управляющий сервер, сервер корреляции и *APM* администратора. К дополнительным компонентам относятся сервер хранения и сервер аналитики.	Автоматизированный мониторинг ИБ и непрерывное отслеживание изменений в ИТ-инфраструктуре организации Автоматизированное обнаружение известных уязвимостей в программном обеспечении активов (требуется дополнительный компонент *Ankey SIEM NG VM*) Выявление инцидентов среди большого количества событий из области ИБ Обнаружение сбоев в работе ИТ- и ИБ-систем и реагирование на них
4	*Kaspersky Unified Monitoring and Analysis Platform*	Представлена на рынке с 2020 г., однако за несколько лет стала одним из лидеров по количеству внедрений в сегменте крупного бизнеса. Является частью экосистемы *Kaspersky Symphony XDR*, куда входят также *Kaspersky EDR Expert, Kaspersky Anti Targeted Attack, Kaspersky ASAP* и другие. Возможность интеграции более чем с 10 отечественными ИБ-системами.	Экосистемность (функциональные интеграции с другими продуктами *Kaspersky*), *RESTful API*, возможность взаимодействия с платформами реагирования (*IRP* и *SOAR*) Автоматизация рутинных действий по реагированию, инвентаризации хостов, обогащению ИБ-событий контекстом Производительность более 500 тыс. EPS, проверенная на реальной архитектуре заказчика Минимальные системные требования и гибкая горизонтальная масштабируемость, поддержка географически распределённой инсталляции, режимы высокой доступности (*high availability*) и мультиарендности (*multi-tenancy*)

№	Наименование программного средства	Краткое описание программного средства	Особенности программного средства
5	*KOMRAD Enterprise SIEM*	Разработка АО «Эшелон Технологии» обладает визуальным конструктором правил корреляции, возможностью автоматизации реагирования на инциденты за счёт использования скриптов на *Bash* и *Python*, встроенной возможностью интеграции с ГосСОПКА.	Возможность автоматизации реагирования на инциденты Визуальный конструктор правил корреляции Наличие постоянно обновляемого пакета экспертиз: бесплатного и расширенного, в рамках действующей технической поддержки Свободно распространяемый дистрибутив с демолицензией
6	*MaxPatrol SIEM*	Является частью линейки продуктов *Positive Technologies*, куда также входят *MaxPatrol VM, PT Network Attack Discovery (PT NAD), MaxPatrol O2, MaxPatrol EDR* и другие. В *MaxPatrol SIEM* реализованы подходы для обеспечения практической результативности мониторинга событий ИБ и управления инцидентами.	Встроенный модуль обнаружения поведенческих аномалий *BAD* (*Behavioral Anomaly Detection*) Инструментарий для обеспечения практической результативности работы аналитика Работа с потоками более 540 тыс. *EPS* Возможность применения в разных ИТ-инфраструктурах – как малых, так и масштаба страны
7	*R-Vision*	Один из самых молодых продуктов на рынке. Он вышел только в 2023 г. При его создании учитывались многолетний опыт R-Vision в разработке технологий, а также трудности, с которыми сталкиваются пользователи при работе с другими *SIEM*-системами.	Возможность расширения функциональности за счёт интеграции с другими технологиями экосистемы *R-Vision EVO* Графический редактор конвейера обработки событий Возможность резервирования по схемам «актив – пассив» и «*N + M*» Гибкая модель хранения данных
8	*RuSIEM*	Одна из старейших российских систем этого класса, отсчитывает свою историю с 2014 г. При необходимости может доукомплектовываться другими продуктами вендора, такими как *RuSIEM IoC, RuSIEM Monitoring, RuSIEM Analytics.*	Микросервисная архитектура Графический конструктор для создания правил корреляции Возможность интеграции со внешними системами за счет использования прикладного интерфейса (*API*) Модуль для работы с активами

Заключение. Использование специальных программных средств в ходе аудита безопасности информационных систем способствует созданию условий для соблюдения требований, предъявляемых к такому процессу, а также способствует его оптимизации и повышению точности его результатов. Основным преимуществом проанализированных программных средств *Efros Defence Operations, Alertix, Ankey SIEM NG, Kaspersky Unified Monitoring and Analysis Platform (KUMA), KOMRAD Enterprise SIEM, MaxPatrol SIEM, R-Vision, RuSIEM* является реализованная в них усовершенствованная функция оценки риска.

Список литературы

1. Бойправ, В. А. Программное средство для проведения аудита системы защиты информации организации / В. А. Бойправ, В. В. Ковалев, Л. Л. Утин // Доклады БГУИР. – 2018. – № 5(115). – С. 44–49.

2. Концепция информационной безопасности Республики Беларусь, утв. постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1

3. Бойправ, В. А. Методика и программное средство для проведения аудита систем менеджмента информационной безопасности / В. А. Бойправ, Л. Л. Утин // Информатика. 2022; 19(4): 42–52.

UDC 004.056

SOFTWARE TOOLS FOR AUDITING THE INFORMATION SYSTEMS SECURITY

Filchenkov P.A.

Master's student of the Department of Information Security, gr.367241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Supervisor: Boiprav O.V. – PhD in Technical Sciences, Associate Professor, Associate Professor of the Department of Information Security

Annotation. The article presents the results of analysis of the most widespread and well-proven in practice software tool for information systems security audit.

Keywords: security audit, information system, software tool, information security risks, security threat.