Технические науки

УДК 004.056

Оладько Владлена Сергеевна
к.т.н., преподаватель
Финансовый университет при Правительстве РФ
г. Москва, Российская Федерация
Пушкарская Анна Игоревна
студент
Волгоградский государственный университет
г. Волгоград, Российская Федерация
Витенбург Екатерина Александровна
аспирант
Волгоградский государственный университет
г. Волгоград, Российская Федерация
Oladko V. S.
Ph.D., Lecture
Financial University under the Government of the RF, Moscow
Pushkarskaya A. I.
Student
Volgograd State University, Volgograd
Vitenburg E. A.
Graduate student
Volgograd State University, Volgograd

ЦЕЛИ И ЗАДАЧИ МОНИТОРИНГА БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

OBJECTIVES AND TASKS OF MONITORING SECURITY IN THE INFORMATION SYSTEM

Аннотация. В статье рассмотрены направления защиты информации в информационной системе организации. Показана необходимость проведения регулярного контроля над состоянием элементов и событиями информационной системы. Представлена схема мониторинга событий и обнаружения инцидентов информационной безопасности в системе. Описаны цели, задачи и уровни мониторинга безопасности информационной системы. Проведен сравнительный анализ мониторинга системного и сетевого уровня.

Ключевые слова: аномалия, события, аудит, инцидент безопасности, защита информации, системный уровень, сетевой уровень, обнаружение атак.

Summary: The article considers the directions of information protection in the information system of the organization. The need for regular monitoring of the elements state and events of the information system is shown. The scheme for monitoring events and detecting incidents of information security is presented. The goals, objectives and levels of monitoring the security of the information system are described. A comparative analysis of system and network level monitoring is carried out.

Keywords: anomaly, events, audit, security incident, information protection, system level, network layer, attack detection.

Анализ приказов и нормативно-методической документации в области защиты информации в информационной системе (ИС) организаций показывает, что при реализации системы защиты (СЗИ) необходимо использовать комплексный подход, построенный на интеграции множества подсистем и механизмов защиты. Организационные и технические меры защиты информации, реализуемые в ИС в рамках ее СЗИ, в зависимости от угроз информационной безопасности (ИБ), используемых информационных

технологий, эксплуатационных и структурно-функциональных характеристик ИС должны обеспечивать [1]:

1) идентификацию и аутентификацию субъектов доступа и объектов доступа в ИС;
2) управление доступом субъектов доступа к объектам доступа в ИС;
3) ограничение программной среды;
4) защиту машинных носителей информации;
5) регистрацию событий безопасности, ведение журналов;
6) антивирусную защиту;
7) обнаружение (предотвращение) вторжений;
8) контроль (анализ) защищенности информации;
9) целостность ИС и информации;
10) доступность информации;
11) конфиденциальность информации и защиту информации от утечек;
12) защиту среды виртуализации;
13) защиту технических средств и программно-аппаратного обеспечения;
14) защиту систем связи и передачи данных ИС.

Часто функции безопасности 5, 7, 8 тесно связаны между собой и используются в едином комплексе, целью которого является регулярный мониторинг состояния безопасности ИС (часто в режиме реального времени) и проведение аудита ИБ, направленного на:

- выявление и прогнозирование событий и инцидентов ИБ;
- оценку уровня текущей защищенности ИС;
- принятие решений по управлению ИБ.

Схема процесса управления обработкой событий ИС в рамках выделенных выше мероприятий по обеспечению безопасности представлена на рисунке 1.

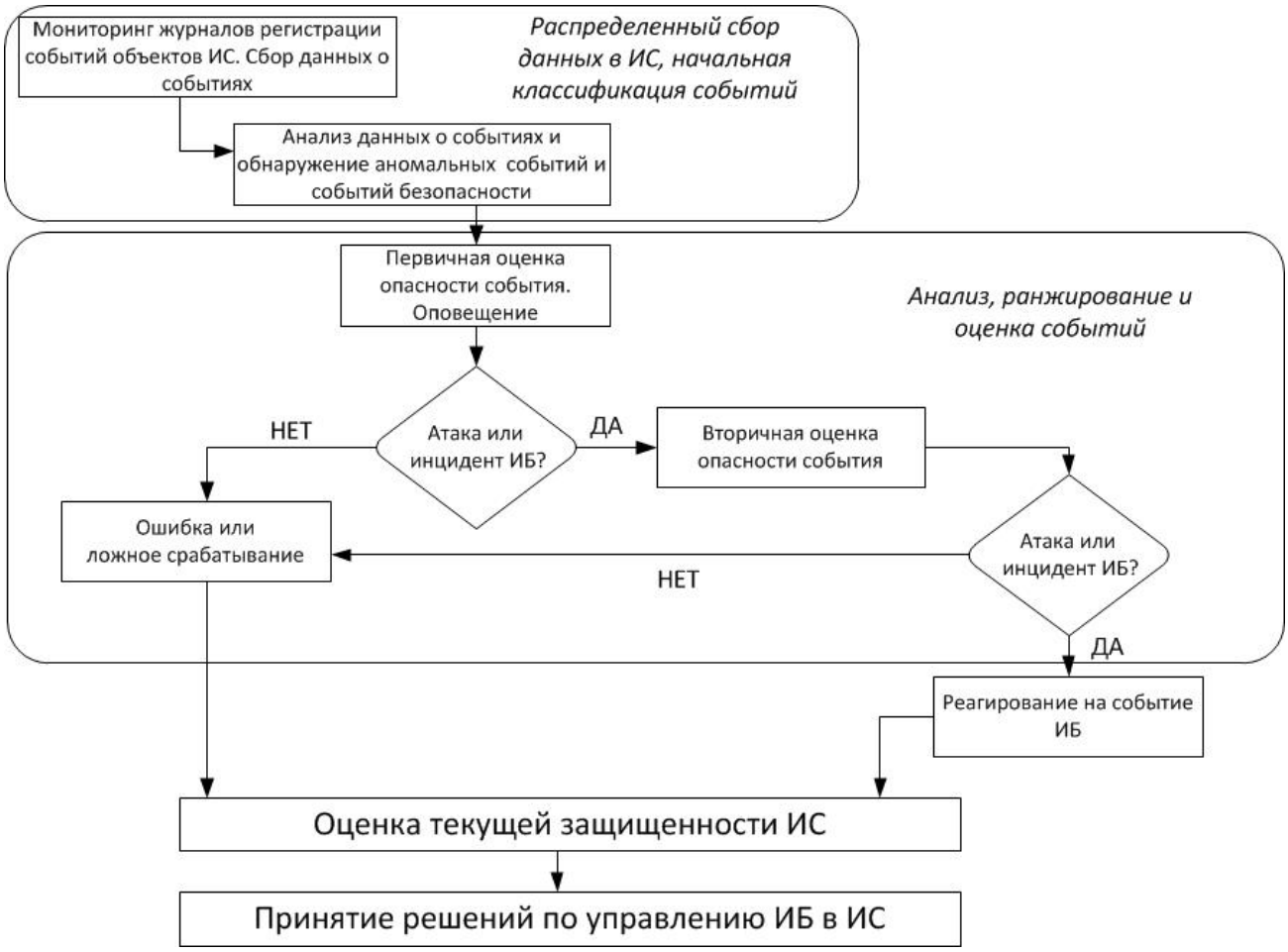

Рис. 1. Мониторинг и обработка событий в ИС

Целью мониторинга безопасности в ИС является наблюдение за средой с целью выявления инцидентов безопасности на базе правил аудита. Задачами мониторинга является:

- сбор данных с подсистем регистрации;
- проверка физической доступности оборудования ИС;
- проверка состояния прикладных и системных служб и сервисов, запущенных в ИС;
- детальная проверка не критичных, но важных параметров функционирования сети: производительности, загрузки, объема и содержания сетевого трафика;

- проверка параметров, специфичных для сервисов и служб данного конкретного окружения;
- контроль дерева и параметров процессов;
- анализ данных и обработка событий и аномалий;
- передача собранных данных в модули выявления инцидентов и аудита безопасности;

Таким образом, назначение систем мониторинга — собирать данные и обнаруживать аномалии в работе ИС, а затем оперативно на них реагировать. Обнаружению подлежит подозрительная и аномальная активность компонентов системы — от пользователей (внутренних и внешних) до программных и аппаратных средств.

Существующие системы мониторинга, используют для обнаружения атак и подозрительной активности в ИС сетевой и системный подход.

При проведении мониторинга на сетевом уровне используют в качестве источника данных для анализа необработанные сетевые пакеты. Для этого используется сетевой адаптер, функционирующий в режиме "прослушивания", и трафик в реальном масштабе времени по мере его прохождения через сегмент сети.

Мониторинг системного уровня контролирует систему, события и журналы регистрации событий безопасности. Когда какой-либо из этих файлов изменяется, то происходит сравнение новых записей с сигнатурами атак, чтобы проверить, есть ли соответствие. Если такое соответствие найдено, то система посылает администратору сигнал тревоги или приводит в действие другие заданные механизмы реагирования.

Каждый уровень проведения мониторинга в ИС имеет свои особенности и охватывает определенную область действия, результаты сравнение возможностей проведения мониторинга на разных уровнях представлено в таблице 1.

Таблица 1 – Сравнение уровней проведения мониторинга в ИС

№	Уровень мониторинга	Вид	Достоинства	Недостатки
1	Системный уровень	Система События Журнал безопасности	подтверждает успех или отказ атаки; контролирует деятельность конкретного узла; обнаруживает атаки, которые упускают системы сетевого уровня; хорошо подходит для сетей с шифрованием и коммутацией; не требуют дополнительных аппаратных средств; низкая стоимость эксплуатации.	зависит от ОС не обнаруживает аномалии возникающие на сетевом уровне
2	Сетевой уровень	Анализ сетевых пакетов	низкая стоимость эксплуатации; обнаруживает атаки или аномалии в поведении, которые возникают на сетевом уровне; обнаруживает и реагирует в реальном масштабе времени; обнаруживает неудавшиеся атаки или подозрительные намерения; не зависит от ОС.	не может обнаруживать атаки системного уровня

Таким образом, недостатки, которые имеются при использовании систем мониторинга только системного уровня, нейтрализуются достоинствами систем мониторинга сетевого уровня и наоборот. Поэтому комбинирование этих двух технологий значительно улучшает эффективность контроля и последующее сопротивление ИС к атакам и злоупотреблениям. По результатам мониторинга безопасности можно выявить потенциальных нарушителей, и закрыть уязвимые места в ИС, что позволит ужесточить политику безопасности и внести большую гибкость в процесс эксплуатации сетевых ресурсов.

Литература:

1. Микова С.Ю., Нестеренко М.А., Белозёрова А.А., Оладько В.С. Состояние и тенденции развития рынка информационной безопасности в Российской Федерации. Actualscience. 2016. Т. 2. № 6. С. 36-39.