УДК 005.21:334.012.42

Никитина Т. О.

ассистент кафедры экономической информатики, учёта и коммерции

Гомельский государственный университет имени Франциска Скорины

Республика Беларусь, г. Гомель

АУДИТ СИСТЕМ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация:

В статье рассматривается аудит систем управления инцидентами информационной безопасности и его значимость в условиях киберугроз. Анализируются ключевые компоненты системы и принципы аудита, помогающие оценить её эффективность. Подчеркивается, что регулярные аудиты выявляют недостатки и способствуют повышению защиты информации в организациях.

Ключевые слова: аудит информационной безопасности, системы управления инцидентами, методы аудита информационной безопасности, принципы аудита информационной безопасности, аудит систем управления инцидентами.

Nikitsina T.

Assistant, Department of Economic Informatics, Accounting and Commerce

Gomel State University named after Francis Skorina

Republic of Belarus, Gomel

AUDIT OF INFORMATION SECURITY INCIDENT MANAGEMENT SYSTEMS

Abstract:

The article examines the audit of information security incident management systems and its importance in the context of cyber threats. The key components of the system and audit principles that help to assess its effectiveness are

analyzed. It is emphasized that regular audits reveal deficiencies and contribute to improving information security in organizations.
Keywords: information security audit, incident management systems, information security audit methods, information security audit principles, audit of incident management systems.

В условиях быстрого развития информационных технологий обеспечение безопасной работы с данными становится одной из ключевых задач современных организаций. Инциденты, такие как несанкционированный доступ и утечка информации, могут нанести серьёзный урон как финансовому состоянию, так и имиджу компании. Поэтому создание надёжных систем управления инцидентами, способных оперативно идентифицировать и реагировать на угрозы, является крайне важным для защиты информационных ресурсов.

Аудит систем управления инцидентами играет значимую роль в оценке их функциональности и соответствия действующим стандартам безопасности. Этот процесс позволяет определить существующие слабые места в реагировании на инциденты и проверить, насколько современные методы адекватны новым киберугрозам.

Аудит инцидентов информационной безопасности представляет собой систематическую проверку и оценку процессов и средств, применяемых для идентификации, обработки и анализа инцидентов, связанных с информационными системами. Основной целью такого аудита является выявление недостатков в управлении инцидентами и обеспечение соответствия действующих процедур современным требованиям безопасности [1].

Система управления инцидентами — это совокупность процессов и технологий, направленных на обнаружение, реагирование и устранение инцидентов информационной безопасности. Важно отметить, что такая

система функционально делится на несколько ключевых компонентов. Первый из них — это идентификация инцидентов, которая включает в себя определение и классификацию нарушений, обнаруженных в информационной системе.

Вторым важным элементом является оперативное реагирование на инциденты. Оно включает в себя реализацию заранее разработанных процедур, направленных на минимизацию негативного воздействия на организацию. Реакция на инциденты требует четкого взаимодействия между различными подразделениями компании, а также высокой степени координации действий, чтобы обеспечить своевременную нейтрализацию угроз.

Системы управления инцидентами также подразумевают элемент восстановления. После устранения источника угрозы важно восстановить нормальное функционирование информационных систем и минимально ухудшить деятельность организации. Этот этап включает в себя анализ причин инцидента и его последствий, что позволяет предотвратить повторение подобных событий в будущем. Эффективное управление инцидентами требует регулярного мониторинга и обновления стратегий, чтобы оставаться актуальным в условиях постоянного изменения киберугроз [2].

Аудит систем управления инцидентами информационной безопасности — это важный процесс, позволяющий оценить текущие механизмы и процедуры, направленные на выявление и реагирование на инциденты. Для успешного проведения такого аудита необходимо следовать установленным принципам и этапам, которые помогут эффективно организовать процесс и получить объективные результаты.

Основные принципы аудита информационной безопасности [3]:

1. Независимость: аудиторы должны оставаться объективными и не уподобляться влиянию сторонних факторов, что обеспечивает достоверность результатов.

2. Объективность: вся информация и факты, собранные в ходе аудита, должны рассматриваться беспристрастно, без предвзятости со стороны аудиторов.

3. Документирование: необходимо фиксировать все этапы аудита и его результаты для дальнейшего анализа и обоснования выводов.

4. Соответствие стандартам: процесс аудита должен быть согласован с общими стандартами и рекомендациями в области информационной безопасности.

5. Постоянное совершенствование: аудит должен служить основой для улучшения текущих процессов и стратегий управления инцидентами.

Этапы аудита систем управления инцидентами:

1. Подготовка к аудиту: сбор информации о текущих процессах управления инцидентами, определение критериев оценки и формирование команды аудиторов.

2. Анализ существующих процедур: оценка действующих методов обнаружения инцидентов, реагирования и восстановления, их документированность и практическая реализация.

3. Проведение оценки рисков: выявление и анализ потенциальных угроз и уязвимостей, способных повлиять на систему управления инцидентами.

4. Интервью и опросы: взаимодействие с персоналом, ответственным за управление инцидентами, для получения мнений о текущих процессах и выявления областей для улучшения.

5. Подготовка отчетов: составление отчетов по результатам аудита, которые содержат рекомендации по улучшению процессов управления инцидентами и повышению уровня безопасности.

6. Реализация рекомендаций: обсуждение отчетов с заинтересованными сторонами и внедрение рекомендованных изменений в практику организации.

7. Мониторинг и пересмотр: регулярная проверка эффективности внедренных улучшений и корректировка процессов в соответствии с текущими угрозами.

Эти принципы и этапы составляют основу методологии аудита систем управления инцидентами. Следование им не только обеспечивает эффективность самих аудитов, но и способствует постоянному совершенствованию процессов управления инцидентами в организациях, что, в свою очередь, позволяет более эффективно реагировать на возникающие угрозы и минимизировать потенциальные риски.

Методология аудита, основанная на четких принципах и последовательных этапах, служит необходимым инструментом для оценки эффективности систем управления инцидентами. Аудит позволяет выявлять недостатки в текущих процессах, а также предоставляет основание для формулирования рекомендаций по их улучшению. Регулярное проведение аудитов является залогом постоянного совершенствования систем управления, что критически важно в условиях стремительно меняющегося ландшафта информационной безопасности.

Использованные источники

1. Скабцов, Н. Kali Linux в действии. Аудит безопасности информационных систем. 2-е издание / Н. Скабцов. – СПб.: Питер, 2024. – 384 с.

2. Дронова, Г.А. Аттестация и аудит информационной безопасности / Г.А. Дронова. – М.: ЛитРес, 2022. – 19 с.

3. Скабцов, Н. Аудит безопасности информационных систем / Н. Скабцов. – СПб.: Питер, 2018. – 272 с.