ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ РАЗРАБОТКИ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО АНАЛИЗА КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

А. П. ТЕЛЕНЬГА

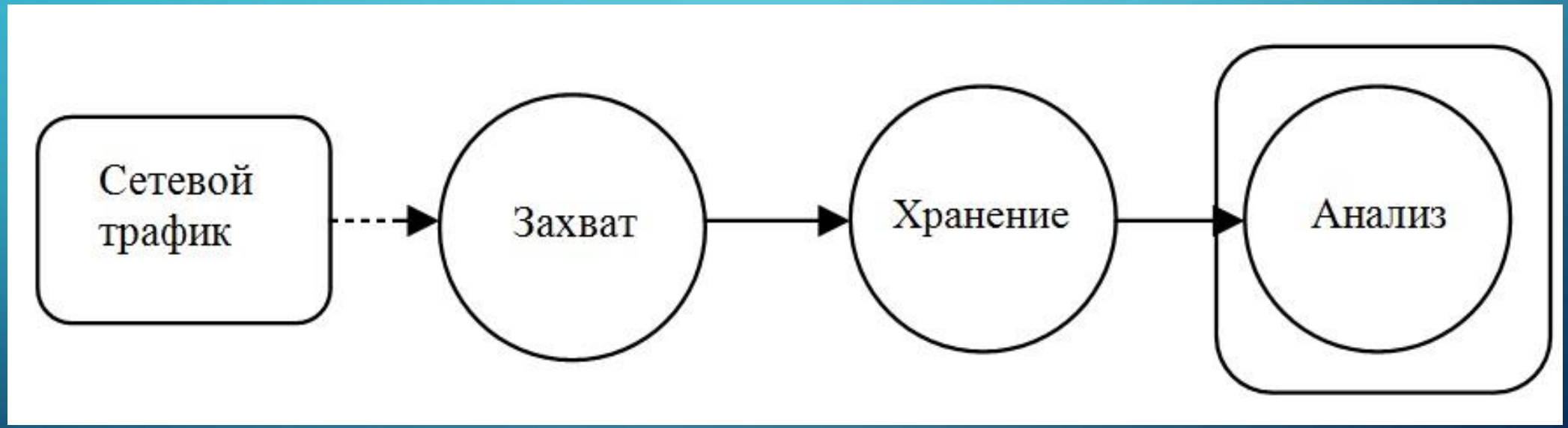
Н. С. ЕВСЕЕНКОВ

КРАСНОДАРСКОЕ ВЫСШЕЕ ВОЕННОЕ ОРДЕНОВ ЖУКОВА И ОКТЯБРЬСКОЙ РЕВОЛЮЦИИ КРАСНОЗНАМЁННОЕ УЧИЛИЩЕ ИМЕНИ ГЕНЕРАЛА АРМИИ С.М. ШТЕМЕНКО

АВТОМАТИЗИРОВАННЫЙ АНАЛИЗ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ. ОПРЕДЕЛЕНИЯ

- Автоматизация – одно из направлений научно-технического прогресса, использующее саморегулирующие технические средства и математические методы с целью освобождения человека от участия в процессах получения, преобразования, передачи и использования энергии, материалов, изделий или информации, либо существенного уменьшения степени этого участия или трудоёмкости выполняемых операций.
- Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.
- Анализ компьютерных инцидентов – это ряд технических мероприятий, направленный на предупреждение, предотвращение, а также расследование аномальных действий в информационной системе, с целью выявить угрозу, которая может нанести существенный ущерб организации, а также деятельность злоумышленников, пытающихся добыть информацию и в дальнейшем использовать её в своих корыстных целях.

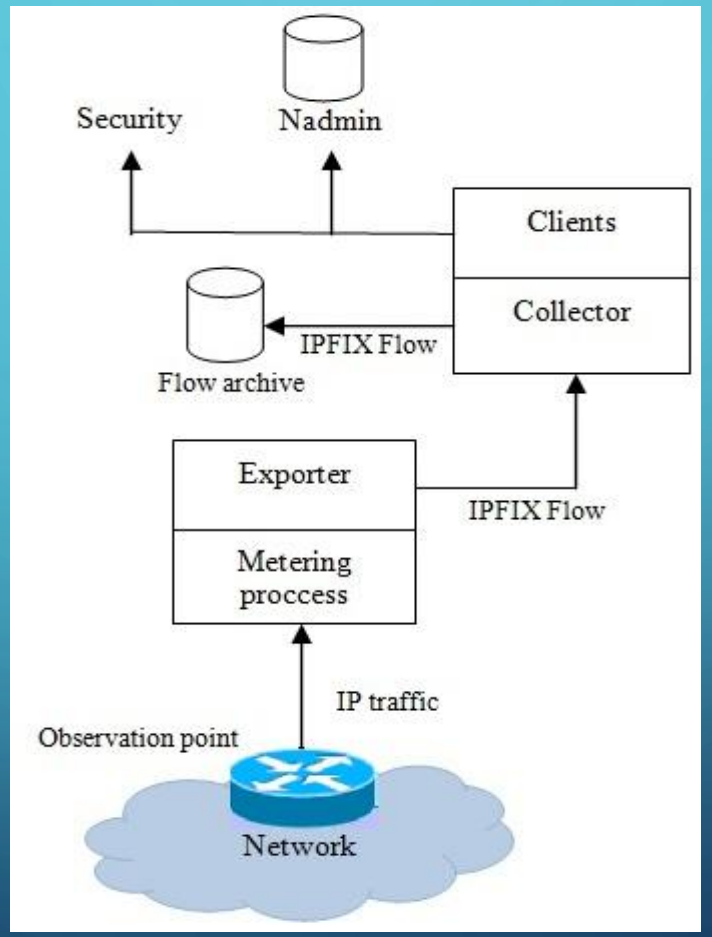
ПОДЗАДАЧИ СИСТЕМЫ АНАЛИЗА СЕТЕВОГО ТРАФИКА



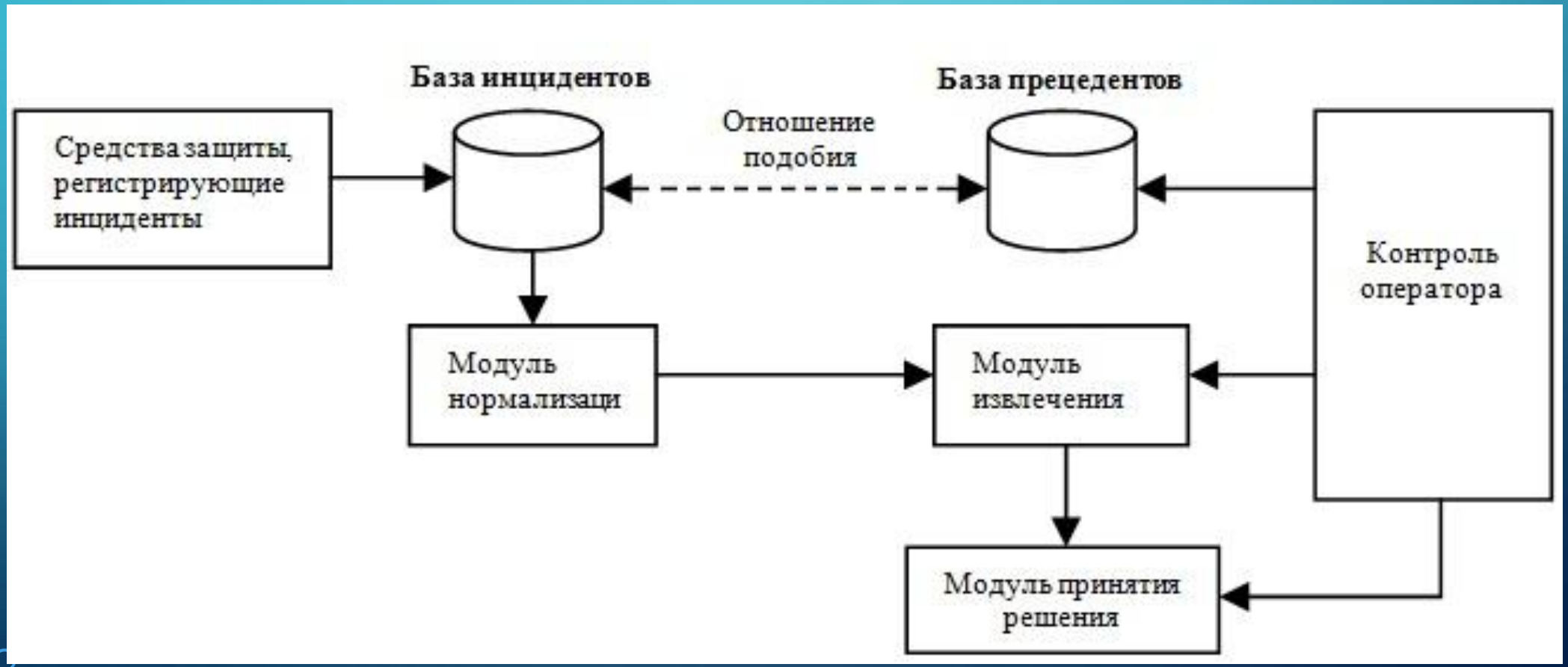
ПРЕДПОСЫЛКИ К ВНЕДРЕНИЮ АВТОМАТИЗИРОВАННОГО АНАЛИЗА КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

- Объем данных. Если над процессом анализа работает только человек, то очевидно, что справиться с таким потоком данных он может только при больших временных затратах, что приводит к снижению эффективности информационной безопасности.
- Потребность в высококвалифицированных специалистах. Для анализа трафика информационной системы и выявления компьютерных инцидентов без участия автоматизации нужны высококвалифицированные работники, хорошо разбирающимися во многих аспектах ИБ, что влечет дополнительные финансовые затраты.

АРХИТЕКТУРА СИСТЕМЫ АНАЛИЗА ТРАФИКА



АРХИТЕКТУРА СИСТЕМЫ ПРЕЦЕДЕНТНОГО АНАЛИЗА



МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРЕЦЕДЕНТНОГО АНАЛИЗА

- Прецедент:

$$CASE = x_1, x_2, \ldots, x_p, R$$

- Аналогия прецедента g и текущей ситуации k:

$$SIM(g,k) = F(sim(x_{g1}, x_{k1}), \ldots, sim(x_{gp}, x_{kp}))$$

- Условие отнесение инцидента к множеству прецедентов:

$$k_j \in G \Leftrightarrow G_l \geq p_{\lim}$$

ЗАКЛЮЧЕНИЕ

- Таким образом, рассмотренная возможность применения прецедентного анализа и его автоматизации при реализации различных стратегий реакции на выявленные инциденты информационной безопасности позволяет нам накапливать базу прецедентов, что впоследствии сокращает время поиска решения для последующих аналогичных происшествий, а также снижает вмешательство человека в процедуру анализа компьютерных инцидентов, тем самым уменьшая риски ошибок 1-го и 2-го рода и повышая защищенность информационной системы в целом