УДК 004.056

# Особенности внедрения SIEM-систем на предприятиях различного типа

А.С. Андреева (Университет ИТМО, г. Санкт-Петербург)

Е.Н. Созинова (Университет ИТМО, г. Санкт-Петербург)

Научный руководитель: Е.Н. Созинова (Университет ИТМО, г. Санкт-Петербург)

Набор средств защиты информации, применяющихся для снижения вероятности реализации угроз информационной безопасности (далее – ИБ), будет отличаться для организаций различного типа в зависимости от объёмов организации, обрабатываемой информации и ряда других немаловажных факторов. В связи с этим существует множество нюансов, которые необходимо учитывать при внедрении SIEM-системы на то или иное предприятие.

Целью работы является проведение анализа моделей построения систем защиты информации в организациях с последующим выявлением особенностей внедрения SIEM-систем на предприятиях различного типа.

Необходимость обеспечивать контроль за конфиденциальностью, целостностью и доступностью информации, как правило, возникает у коммерческих организаций, к которым относятся такие виды предприятий как:

- хозяйственные товарищества и общества;
- производственные кооперативы;
- государственные и муниципальные унитарные предприятия.

Построение системы защиты информации для данных организаций будет основано не только на том, какая информация создаётся, обрабатывается, передаётся и хранится в рамках осуществления основного вида деятельности предприятия и какие угрозы для неё будут характерны, но также и на том, как должна функционировать IT-инфраструктура внутри компании, поскольку в зависимости от вида деятельности важность обеспечения конфиденциальности, целостности и доступности будет различаться для фирмы, занимающейся торговлей и для учебного заведения.

SIEM-система, как система ИБ и управления событиями, является тонким инструментом администратора ИБ предприятия, которая предназначена для решения таких задач как, например:

- консолидация данных;
- корреляция и обработка событий безопасности;
- предоставление инструментов для экспертного анализа;
- оповещение администратора безопасности об инцидентах;
- хранение событий безопасности;
- и др.

С помощью SIEM-системы становится возможным провести анализ событий, происходящих в сети предприятия и в соответствии с тем, какие инциденты ИБ могут привести к реализации угроз, а какие не являются таковыми инцидентами, производятся настройки данной системы, которые для предприятий одного типа будут иметь характерные особенности.