Якунин А.Д.
Канд. тех. наук Макаров К.В.
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
alekyakuninmus@gmail.com

Разработка политики информационной безопасности предприятия.

В современных условиях всеобщей информатизации и развития информационных технологий усиливаются угрозы информационной безопасности промышленных предприятий.

Стратегия развития промышленных предприятий требует непрерывного совершенствования производственной инфраструктуры для успешного проникновения на новые рынки сбыта, решения вопросов повышения эффективности взаимодействия с поставщиками и потребителями. Для этого необходимо создание различных подразделений в структуре самой организации и постоянное усложнение и совершенствование информационной системы с необходимостью применения новых информационных технологий (ИТ).

При расширении автоматизированной информационной системы, существенно возрастает вероятность внешних и внутренних угроз, которые направлены на подрыв информационной безопасности промышленного предприятия и утечки персональной и конфиденциальной информации.

По данным Positive Technologies [1], корпоративные сети более 70% промышленных предприятий потенциально уязвимы при атаках хакеров. К таким выводам пришли аналитики, проведя исследование векторов атак на корпоративные информационные системы промышленных компаний.

На предприятии хранится и обрабатывается огромное количество различных данных, связанных с конструкторскими разработками и технологиями оптимизации производства, а так же персональные данные сотрудников, служебная и иная конфиденциальная информация[2].

Под информационной безопасностью предприятия понимается организованная совокупность мер, средств, методов и мероприятий, снижающих уязвимость конфиденциальной информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке.

Для успешного и эффективного функционирования предприятия необходимо внедрение комплексных мер по обеспечению информационной безопасности.

Целью работы является разработка комплекса мер по защите конфиденциальных данных предприятия. Для её достижения требуется выполнить следующие задачи:

1. Произвести общий анализ угроз предприятия;
2. Сформировать модель угроз ИБ;
3. Сформировать модель защиты конфиденциальных данных предприятия;
4. Выбрать наиболее рациональное решение задач ИБ;
5. Реализовать выбранное решение.

Итогом работы должен являться набор политик, обеспечивающих защиту конфиденциальных данных предприятия.

Литература

1. Концепция национальной безопасности РФ, утверждена Указом Президента РФ от 17.12.97 г. № 1300 (в ред. Указа Президента РФ от 10.01.2000 г. № 24).

2. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ.