УДК 65.012.45

магистр Е.В. Брусенцова
ГВУЗ «Национальный горный университет»

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

В данной статье рассматриваются принципы системы информационной безопасности, а также цели, которые преследует система защиты информации на предприятии.

Безопасность информации предполагает отсутствие недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на ресурсы, используемые в автоматизированной системе. Критериями информационной безопасности являются конфиденциальность, целостность и будущая доступность информации.

Следует подчеркнуть, что темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы. Поэтому решение вопроса о разработке эффективной политики информационной безопасности на современном предприятии напрямую связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации.

Современные методы управления рисками позволяют решить ряд задач перспективного развития предприятия. Во-первых, количественно оценить текущий уровень информационной безопасности предприятия, что потребует выявления рисков. Во-вторых, в систему риск-менеджмента на предприятии может быть включена политика безопасности и планы совершенствования корпоративной системы защиты информации для достижения приемлемого уровня защищенности информационных активов компании.

С этой целью рекомендуется осуществить расчет финансовых вложений в обеспечение безопасности на основе технологий анализа рисков, произвести соотношение расходов на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения. Необходимо

выявлять и проводить первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы. Следует определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности предприятия, а также разработать необходимый пакет организационно-распорядительной документации. Одновременно следует осуществлять разработку и согласование со службами предприятия, надзорными органами проекта внедрения необходимого комплекса защиты, учитывающего современный уровень и тенденции развития информационных технологий. Кроме того, важным мероприятием поддержки системы безопасности информации является обеспечение поддержания внедренного комплекса защиты в соответствии с изменяющимися условиями работы предприятия, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

Система защиты информации на предприятии преследует такие цели как предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Помимо этого система информационной безопасности нацелена на обеспечение устойчивого функционирования объекта: предотвращение угроз его безопасности, защиту законных интересов владельца информации от противоправных посягательств.

Обязательным условием эффективной реализации вышеупомянутых целей является непременный контроль качества предоставляемых услуг и обеспечение гарантий безопасности имущественных прав и интересов клиентов.

В связи с этим, система информационной безопасности должна базироваться на следующих принципах:

– прогнозирование и своевременное выявление угроз безопасности информационных ресурсов, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

– создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;

– создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;

– создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц и, тем самым, ослабление возможного негативного влияния последствий нарушения информационной безопасности.

Перечень литературы:

1. «Информационная безопасность предприятия» - Конев И.З., Беляев А.В., СПб.: БХВ-Петербург, 2003;

2. «Основы информационной безопасности» - Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов, Горячая Линия - Телеком.