УДК 004:[005.1+005.3]

студентка И.С. Корецкая, асс. М.В. Торбеева
ГВУЗ «Национальный горный университет»

ПОСТРОЕНИЕ ЕФЕКТИВНОЙ СИСТЕМЫ ОЦЕНКИ И УПРАВЛЕНИЯ РИСКАМИ

В данном докладе проведен анализ проблемы эффективного управления рисками информационной безопасности на предприятии.

Полноценное обеспечение информационной безопасности(ИБ) требует применения комплексного подхода к анализу информационной системы компании, который будет максимально полно учитывать все многообразие форм представления и способов обработки, хранения и передачи информации. Важную роль в этой системе играет управление и анализ рисков, а именно разграничение приемлемых и неприемлемых рисков информационной безопасности.

При определении рисков ИБ возникает достаточно объемный перечень. Встает вопрос, необходимости защиты от всех рисков. Данный вопрос решаются очень просто, если при определении и оценке риска учитывать три параметра: угроза (вероятность отрицательного воздействия), уязвимость (уровень текущей защиты от отрицательного воздействия), убыток (нанесение урона или создание такой возможности). Угрозы для организации исходят как изнутри (недовольные сотрудники), так и снаружи (недостаточно эффективная система защиты от внешних воздействий). Уязвимости возникают из-за неэффективного управления компанией и недоработок в информационных системах.

Проведение анализа информационных рисков и оценка защищенности информации играют важную роль, так как именно они и позволяют определить ценность информационных ресурсов и оценить эффективность затрат на защиту информации. Для выделенных информационных ресурсов следует определить их стоимость или ценность как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности,

нематериального ущерба от разглашения конфиденциальной информации и т.д. При этом оценку можно производить по качественной шкале, определяя уровень критичности информации (например, низкий, средний, высокий), однако получение стоимости ресурса в денежном выражении позволяет дать существенно более точную оценку, а результат в этом случае становится более наглядным, в том числе и для неспециалиста в области защиты информации. [3]

Оценивая риски, получают перечень особо опасных рисков, к минимизации которых необходимо приступать немедленно, что, в свою очередь, значительно повысит уровень информационной безопасности организации. Уменьшение остальных рисков, как правило, не требуется, поскольку мероприятия по их снижению могут иметь малую эффективность по сравнению с затрачиваемыми ресурсами. Поэтому основной задачей является определение логической границы между опасными и допустимыми рисками. В начале построения системы ИБ данная граница может иметь высокий уровень, дальнейшее понижение этой границы возможно при проведении работ по ИБ, но необходимо определить тот момент, когда ее дальнейшее снижение станет убыточным для организации. Иначе возможен переход в состояние, когда мероприятия по защите информации будут работать сами на себя. Для оценки данной границы необходимо четко оценивать свои ресурсы и возможные расходы. [1]

Для повышения эффективности управления рисками ИБ необходимо решить две задачи оптимизации:

1. Задачу определения оптимального объема денежных средств, необходимого для достижения требуемого уровня ИБ на предприятии;

2. Задачу оптимального распределения денежных средств между отдельными направлениями защиты информации ИБ, при котором значение информационного риска для организации в целом будет минимально.[3]

Соответственно из всего выше сказанного можно сделать выводы, что именно определение логической границы между опасными и допустимыми

рисками, а также решение задач оптимизации являются необходимыми условиями для эффективного управления информационными рисками.

Перечень литературы:

1. http://www.management.com.ua/finance/fin097.html
2. http://www.connect.ru/article.asp?id=8910
3. http://iso27000.ru/sobytiya/copy2_of_master-klass-upravlenie-riskami-informacionnoi-bezopasnosti-v-sootvetstvii-s-trebovaniyami-mezhdunarodnogo-standarta-iso-27001