Г.Е. Шепитько, Г.Н. Гудов

РАСЧЁТ ЭКОНОМИЧЕСКОГО РИСКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

В области информационной безопасности накоплен многолетний опыт защиты государственной тайны в государственных структурах, который базируется на исполнении директивных указаний в нормативных документах. В последнее десятилетие появился новый класс обладателей информации – класс собственников акционерских обществ, защита информации которых имеет свои особенности.

Во-первых, наблюдается устойчивая тенденция государства переложить проблемы защиты информации на собственников акционерных обществ. Во-вторых, собственники акционерных обществ вынуждены учитывать экономическую эффективность затрат на защиту коммерческой тайны, что порой приводит к необоснованному игнорированию части нормативных требований по защите информации.

В перспективе новый импульс в развитии должен получить метод технико-экономического обоснования проектов систем информационной безопасности с использованием всего спектра средств и мероприятий по защите информации [1]. По существу планируется в будущем реализовать концепцию допустимого риска в области информационной безопасности в соответствии с определением безопасности в ст.1 ФЗ "О техническом регулировании" № 184-ФЗ от 27.12.2002 г. как состояния, при котором отсутствует недопустимый риск, связанный с причинением вреда государственному или муниципальному имуществу, имуществу физических или юридических лиц.

Рассмотрим частную задачу расчёта экономического риска системы информационной безопасности, когда объектом защиты является автономный компьютер, установленный в отдельном помещении, а предметом защиты – информация на его электронных носителях.

Будем считать, что информация в зависимости от её стоимости может быть отнесена к одной из четырёх категорий важности, в соответствие которой поставлены следующие виды нарушителей и рубежи защиты:

- на информацию 4-й категории важности в основном посягают ***случайные*** внутренние нарушители (пользователи персональных компьютеров), для противодействия которым достаточно первого рубежа защиты с использованием организационно-правовых мероприятий;

- на информацию 3-й категории важности посягают ***неквалифицированные*** нарушители (пользователи специальных программ с целью хищения носителей информации), для противодействия которым недостаточно

первого рубежа защиты и приходится устанавливать 2-й рубеж защиты с использованием физических средств защиты;

- на информацию 2-й категории важности посягают ***квалифицированные*** нарушители (способные программисты с целью несанкционированного доступа к информации), для противодействия которым приходится устанавливать дополнительно 3-й рубеж защиты с использованием программных средств защиты;

- на информацию 1-й категории важности посягают ***высококвалифицированные*** внешние нарушители (квалифицированные программисты и специалисты по вычислительной и специальной технике с целью несанкционированного доступа к информации), для противодействия которым приходится устанавливать дополнительно 4-й рубеж защиты с использованием аппаратных и аппаратно-программных средств защиты.

Примем, что в зависимости от квалификации нарушитель может использовать ***S*** контролируемых каналов несанкционированного доступа (НСД) к информации на компьютере, тогда вероятность защиты компьютера определяется по следующей формуле:

$$P_{зj} = \sqrt[S+1]{(1 - P_{обхк}) \prod_{q=1}^{S} P(q)},$$

где $P_{обхк}$ – вероятность обхода нарушителем контролируемых каналов НСД к объекту защиты;

S – количество контролируемых каналов НСД к объекту защиты;

$P(q)$ – вероятность защиты объекта для q-го канала НСД к объекту защиты, определяемая соотношением

$$P(q) = 1 - \prod_{n=1}^{4} P\left[(1 - P_n) \cdot (1 - P_{обхр}) + P_{обхр}\right],$$

$P_{обхр}$ – вероятность обхода нарушителем n-го рубежа защиты;

P_n – вероятность защиты объекта n-м рубежом защиты (организационно-правовыми, физическими, программными и аппаратными средствами защиты):

$$P_n = 1 - \prod_{t=1}^{m} (1 - P_t),$$

P_t – вероятность защиты объекта при использовании t -го средства (мероприятия) на одном рубеже защиты.

Тогда с учётом (1) можно записать выражение для экономического риска информационной безопасности [2]

$$R_э = Ц_{кт} \cdot P_l \cdot P_e \cdot V_z \cdot P_z \cdot P_{кзи},$$

где $Ц_{кт}$ – стоимость информации, содержащей коммерческую тайну;

P_l – вероятность проявления l-го вида источников угроз (внутренний нарушитель, внешний нарушитель);

P_e – вероятность проявления e-го источника угроз (высоко квалифицированный, квалифицированный, неквалифицированный или случайный нарушитель);

P_z – вероятность проявления z-й угрозы (утечка, модификация или утрата информации);

V_z – доля ущерба от реализации z-й угрозы;

$P_{кзи}$ – условная вероятность отсутствия защиты объекта многорубежной системой защиты от всех d способов реализации угроз (ознакомление, разглашение, фальсификация, кража, блокировка, потеря информации), определяемая соотношением

$$P_{кзи} = \sum_{j=1}^{d} P_j (1 - P_{зj}),$$

P_j – вероятность проявления j-го способа реализации угрозы;

Полученное значение $R_э$ экономического риска информационной безопасности сравнивается с допустимым значением

$R_{эд} = Ц_{кт} \cdot \beta$,

где β – значение ставки риска безопасности, которое обычно не превышает нескольких процентов.

При невыполнении условия достаточности уровня защиты информации необходимо для усиления рубежей защиты добавить мероприятия или средства защиты.

$$R_э \le R_{эд}.$$

Использование предложенных формул расчёта позволит обосновать уровень защиты информации, при котором отсутствует недопустимый риск безопасности информации.

Литература

1. Гудов Г.Н., Шепитько Г.Е. Защита конфиденциальной информации в акционерных обществах: Учебное пособие. -М.: Академия экономической безопасности МВД России, 2006. –290 с.

2. Шепитько Г.Е., Медведев И.И. Проблемы безопасности объектов: Учебное пособие. -М.: Академия экономической безопасности МВД России, 2006. –200 с.