УДК 004.492.2

АНАЛИЗ МОДЕЛИ ДЛЯ ОЦЕНКИ ПОТЕРЬ, СВЯЗАННЫХ С РЕАЛИЗАЦИЕЙ УГРОЗ И СТРАХОВАНИЕМ ИНФОРМАЦИОННЫХ РИСКОВ

Е.Д.Никуленко, Н.Е.Губенко
Донецкий национальный технический университет
elena.nikulenko@gmail.com

Рассмотрены понятия информационных потерь, видов угроз информации, страхования информационных рисков. Представлены формулы для расчета оценки потерь от угроз свойствам информации, формулы для расчета потерь с использованием страхования рисков.

Разработка модели оценки потерь является актуальной задачей потому, что соединяет воедино цели руководства по увеличению прибыли предприятия с задачей отдела информационной безопасности (ИБ) по уменьшению потерь, связанных с проблемами защиты главных свойств информации (доступности, целостности, конфиденциальности).

Угроза доступности – это ограниченность доступа к ресурсу или полное его отсутствие, которое может произойти как в случаи преднамеренного, так и случайного действия. Если доступ к ресурсу имеется, но при этом происходит с затратой большого промежутка времени, говорят что ресурс исчерпан.

Формула для расчета потерь от угроз доступности: $L = L_{ul} + L_r + L_d + L_{li}$, где L_{ul} – потери от несвоевременного оказания услуг по доступу к информации; L_r – потери, связанные с восстановлением работоспособности; L_d – потери, связанные с простоем узла системы (УС); L_{li} – потери, связанные с потерей дохода [1]. Потери от несвоевременного оказания услуг по доступу могут быть зафиксированы в договоре по эксплуатации и представлять неустойку и возмещение ущерба.

Потери, связанные с восстановлением работоспособности рассчитываются:

$$L_r = \frac{\sum_{i=1}^{N} S_i}{T} * t_r \qquad (1),$$

где S_i — зарплата в месяц сотрудника, восстанавливающего работоспособность атакованного узла системы (АУС); N — количество сотрудников, восстанавливающих работоспособность

АУС; t_r — время восстановления работоспособности; T — количество рабочих часов узла системы в месяц [1].

Потери, связанные с простоем АУС рассчитываются по формуле $L_d = \frac{\sum_{i=1}^{N} S_i}{T} * t_d$, где S_i — зарплата в месяц сотрудника АУС; N — количество сотрудников АУС; t_d — время простоя АУС; T — количество рабочих часов узла системы в месяц [1].

Потери, связанные с потерей дохода определяются по формуле $L_{li} = Inc * \frac{t_r + t_d}{T}$, где Inc – годовой доход от использования АУС; t_r — время восстановления АУС; t_d — время простоя АУС; T — период работы системы в течение года [1].

Понятие «целостность» говорит, что данные полны и неизменны. Данные могут быть подвержены изменениям преднамеренно и непреднамеренно. Для угроз целостности потери могут быть подсчитаны по формуле $L = L_{um} + L_r + L_d + L_{li}$, где L_{um} — потери от несанкционированной модификации информации, размер потерь будет зависеть от значимости информации, целостность которой нарушена; L_r — потери, связанные с восстановлением работоспособности; L_d — потери, связанные с простоем узла системы; L_{li} — потери, связанные с утратой возможного дохода [1].

Сумма потерь, связанных с восстановлением работоспособности рассчитывается по следующей формуле $L = L_{ri} + L_{rc}$, где L_{ri} — потери, связанные с восстановлением информации; L_{rc} — потери, связанные с заменой поврежденных компонент, являются фиксированными материальными затратами [1].

Потери, связанные с восстановлением информации, могут быть рассчитаны следующим образом $L_{ri} = \frac{\sum_{i=1}^{N} S_i}{T} * t_{ri}$, где S_i — зарплата в месяц сотрудника атакованного узла системы; N — количество сотрудников на атакованном узле системы; t_{ri} — время, необходимое для восстановления информации на атакованном узле системы; T — количество рабочих часов узла системы в месяц [1].

Потери, связанные с простоем АУС рассчитываются по формуле 1.

Потери, связанные с утратой возможного дохода, определяются по формуле: $L_{li} = Inc * \frac{t_d + t_r + t_{ri}}{T}$, где Inc — годовой доход АУС; t_d — время простоя АУС; t_r — время восстановления АУС; t_{ri}— время

восстановления информации на атакованном АУС; T — период работы системы в течение года [1].

Конфиденциальность информации — это необходимость предотвращения утечки (разглашения) какой-либо информации. При этом при разглашении информации, ее владелец будет иметь потери, которые могут быть связаны с финансовой стороной вопроса, потерей репутации, конкурентоспособности и т.д. Поэтому конфиденциальная информация подразумевает право пользования ею только ограниченного числа лиц, для остальных она остается тайной [2].

Главной задачей при оценке потерь для конфиденциальности информации является само присвоение информации статуса «конфиденциальной».

Поэтому для расчета потерь наиболее удобным является метод экспертных оценок. Сущность метода заключается в том, что группа специалистов в данной области и анализируют потери, исходя из значимости самой информации.

Страхование информационных рисков предприятия — это метод защиты информации в рамках финансово-экономического обеспечения системы защиты информации, основанный на выдаче страховыми обществами гарантий субъектам информационных отношений по восполнению материального ущерба в случае реализации угроз информационной безопасности [3].

С использованием страхования информационных рисков предприятия итоговые потери (L*) рассчитываются по формуле $L^* = L - Ins$, где L — суммарные потери из-за нарушения нескольких категорий информации; Ins — суммарная прибыль от страхование рисков, которая рассчитывается по формуле $Ins = Ins_f + Ins_{ob} + Ins_{bil} + Ins_{tran}$, где Ins_f — доход от страхования средств защиты информации; Ins_{ob} — доход от страхования объектов защиты информации; Ins_{bil} — доход от страхования помещений и зданий, где хранится информация; Ins_{tran} — доход от страхования средств передачи информации [1].

Кроме того, на суммарные годовые информационные потери влияет денежная инфляция. Инфляция побуждает нерадивых, ищущих легких денег сотрудников заниматься компьютерными преступлениями, в том числе продажей конфиденциальной информации.

Расчет темпов инфляции базируется на следующих данных: прогноза социально-экономического развития страны, который ежегодно предоставляется правительством в парламентские структуры и публикуется в печати; проекта государственного и

регионального бюджетов на предстоящий год, в котором дается оценка инфляции, учитываемой в бюджетных расчетах; расчета Национального банка о возможных темпах инфляции; прогнозные данные по курсу доллара, т. к. в настоящее время экономика России привязана к этому показателю; оценки экспертов (научных организаций и др.) [4].

Если страхования рисков уменьшает информационные потери, то инфляция наоборот увеличивает, что представлено на рисунке 1, потому что стимулирует увеличение цен на приобретение и ремонт оборудования, а также оплату труда сотрудников,

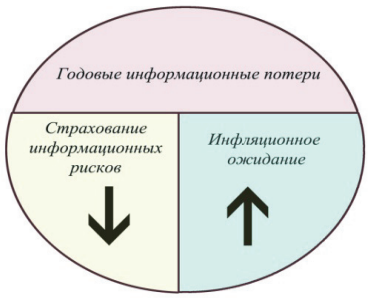

Рисунок 1 – Зависимость годовых потерь от страхования и инфляции

Таким образом, как показывает приведенный анализ, к существующим моделям и методам оценки целесообразно добавить страхование информационных рисков и оценку темпов инфляции.

Список литературы

1. Гроздов, Г. Г. Способ решения задачи формирования комплексной системы защиты информации для автоматизированных систем 1 и 2 класса [Текст] / Г. Г. Гроздов // (Препринт/ НАН Украины. Отделение гибридных управляющих систем в энергетике ИПМЭ им. Г. П. Пухова НАН Украины; № 01/2005) – Киев : ЧП Нестреровой, 2005. – С. 66.
2. Тимошенко, А. А. Защита информации в специализированных информационно-телекоммуникационных системах – Текст лекции, Киев, 2010.
3. «Амулет» [Electronic resourse] / Интернет-ресурс. – Режим доступа к статье: http://www.amulet-group.ru/page.htm?id=30 – Страхование информационных рисков как метод защиты информации. Д. Дьяконов.
4. "UniverLib." [Electronic resourse] / Интернет-ресурс. – Режим доступа к статье: http://www.univerlib.ru/page/57-ustanovlenije-okonchatelynoj-ceny-2911.html – Установление окончательной цены.

Получено 12.09.2011