УДК 004.492.2

АНАЛИЗ МОДЕЛИ ДЛЯ ОЦЕНКИ ПОТЕРЬ, СВЯЗАННЫХ С РЕАЛИЗАЦИЕЙ УГРОЗ И УЯЗВИМОСТЕЙ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Губенко Н.Е., Никуленко Е.Д.
Донецкий национальный технический университет
Кафедра компьютерных систем мониторинга
E-mail: elena.nikulenko@gmail.com

Аннотация

Губенко Н.Е., Никуленко Е.Д. Анализ модели для оценки потерь, связанных с реализацией угроз и уязвимостей для информационных систем*. Рассмотрены понятия и классы угроз и уязвимостей для информационных систем. Представлены формулы для расчета оценки потерь от угроз, нарушающих одно или несколько свойств информации.*

Общая постановка проблемы

Основная цель каждого коммерческого предприятия – принесение прибыли своим владельцам. Потери, связанные с удалением, утечкой, модификацией информации предприятия приобрели масштабный характер. Причины этому могут быть различные, начиная от конкурентной борьбы и закачивая личными конфликтами сотрудников. Цель построения модели оценки потерь – обнаружение и устранение уязвимостей на предприятии.

Модель оценки потерь предполагает расчет убытков от слабых мест системы, идентификацию существующих угроз безопасности и уязвимостей.

Каждой из составляющих информационной безопасности (конфиденциальность, целостность и доступность) соответствуют свои формулы расчета потерь.

Так как компания несет убытки исключительно из-за потери ценной информации, одним из ключевых моментов составления модели потерь являются причины, которые эти потери предполагают. Причинами потерь являются внешние угрозы и уязвимости самой системы. Модель реализации угрозы проходит по следующему пути: источник угрозы – фактор (уязвимость) – угроза (действие) – последствия (атака) [1].

«Угроза» в информационной безопасности представляет собой понятие доступа к секретным информационным ресурсам, не имея юридических прав на них.

Уязвимость – слабое место системы, влияя на которую, угроза может принести реальный вред системе.

В настоящий момент распространены несколько методик оценки потерь. В данной работе остановимся подробнее на оценке потерь для угроз доступности, целостности и конфиденциальности в соответствии с подходом, предложенным Гроздовым в работе 1.

Подход к оценке потерь для угроз доступности

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:

$$L = L_{лт} + L_{в} + L_{п} + L_{пд}; \quad (1)$$

где $L_{лт}$ – потери от несвоевременного оказания услуг по доступу к информации; $L_{в}$ – потери, связанные с восстановлением работоспособности; $L_{п}$ – потери, связанные с простоем узла системы; $L_{пд}$ – потери, связанные с потерей дохода [2].

Потери от несвоевременного оказания услуг по доступу могут быть зафикисрованы в договоре по эксплуатации и представлять неустойку и возмещение ущерба.

Потери, связанные с восстановлением работоспособности рассчитываются:

$$L_в = \frac{\sum_{i=1}^{Nc} Zc_i}{T} * t_в; \quad (2)$$

где Zc_i - зарплата в месяц сотрудника, восстанавливающего работоспособность атакованного узла системы; N_c - количество сотрудников, восстанавливающих работоспособность атакованного узла системы; $t_п$ - время восстановления работоспособности; T - количество рабочих часов узла системы в месяц [2].

Потери, связанные с простоем атакованного узла:

$$L_п = \frac{\sum_{i=1}^{Nc} Zc_i}{T} * t_п; \quad (3)$$

где Zc - зарплата в месяц сотрудника атакованного узла системы; N_c - количество сотрудников на атакованном узле системы; $t_п$ - время простоя узла системы; T - количество рабочих часов узла системы в месяц [2].

Потери, связанные с потерей дохода определяются по такой формуле:

$$L_{пд} = D * \frac{t_п + t_в}{T}; \quad (4)$$

где D – годовой доход от использования атакованного узла системы; $t_п$ - время простоя атакованного узла системы; $t_в$– время восстановления атакованного узла; T - период работы системы в течении года [2].

К категории наиболее небезопасных угроз следует отнести непреднамеренные ошибки лиц, которые имеют неограниченный доступ к информационной системе.

Подход к оценке потерь для угроз целостности

Понятие «целостность» говорит, что данные полны и неизменны. Данные могут быть подвержены изменениям преднамеренно и непреднамеренно. Непреднамеренное изменение включает в себя сбои, отказы системы, ошибки ввода и другие. Преднамеренное – несанкционированный доступ, который происходит вследствие умышленного изменения информации с целью получения выгоды, может быть реализовано как посторонними, так и уполномоченными лицами.

Для угроз целостности потери могут быть подсчитаны по формуле:

$$L = L_{нм} + L_в + L_п + L_{пд}; \quad (5)$$

где $L_{нм}$ — потери от несанкционированной модификации информации. Размер потерь будет зависеть от значимости информации, целостность которой нарушена; $L_в$ — потери, связанные с восстановлением работоспособности; $L_п$ — потери, связанные с простоем узла системы; $L_{пд}$ — потери, связанные с утратой возможного дохода [2].

Сумма потерь, связанных с восстановлением работоспособности рассчитывается по следующей формуле:

$$L_в = L_{нм} + L_{вр} + L_{ви} + L_{зк}; \quad (6)$$

где $L_{ви}$ - потери, связанные с восстановлением информации; $L_{вр}$ — потери, вязанные с восстановлением работоспособности; $L_{зк}$ — потери, связанные с заменой поврежденных компонент [2].

Потери, связанные с восстановлением информации, могут быть рассчитаны следующим образом:

$$L_{ви} = \frac{\sum_{i=1}^{Nc} Zc_i}{T} * t_{ви}; \quad (7)$$

где Zc_i — зарплата в месяц сотрудника атакованного узла системы; N_c — количество сотрудников на атакованном узле системы; $t_{ви}$ — время, необходимое для восстановления

информации на атакованном узле системы; T - количество рабочих часов узла системы в месяц [2].

Потери, связанные с утратой возможного дохода, определяются по формуле:

$$L_{пд} = D * \frac{t_п + t_в + t_{ви}}{T}; \quad (8)$$

где D - годовой доход атакованного узла системы; $t_п$ — время простоя атакованного узла системы; $t_в$ — время восстановления атакованного узла системы; $t_{ви}$ — время восстановления информации на атакованном узле системы; T — период работы системы в течение года [2].

Потери и угроза конфиденциальности

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 [3]. Таким образом, проанализировав потери от угроз конфиденциальности, был сделан вывод, что эти потери варьируется от показателя значимости самой информации.

Оценка потерь, которые нарушают несколько свойств информации, может быть различной именно от свойств, которые были подвергнуты угрозе.

Схематичное представление модели оценки потерь

Модель оценки потерь не является обособленной, а является составной частью общей модели защиты информации.

Представление модели оценки потерь представлено на рисунке 1. Финансовые потоки предприятий чаще всего постоянны, и наличие потерь не дает возможность вкладывать утерянные деньги в дальнейшее производство.

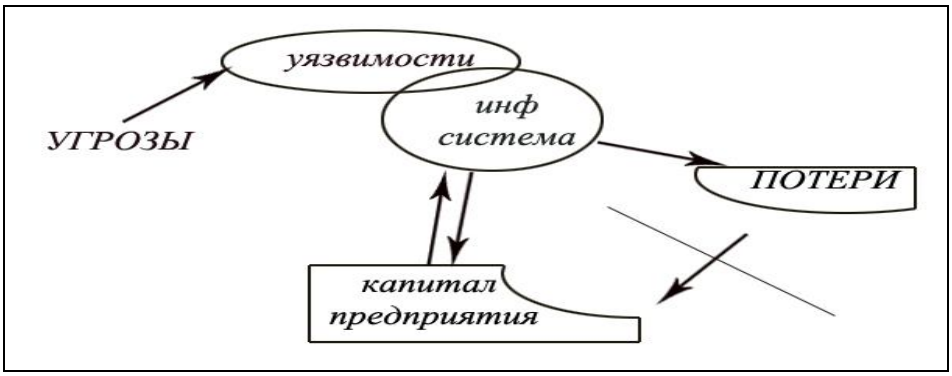

Рис 1. Представление модели оценки потерь

Применение результатов расчета

В целом, модель расчета потерь строится на приведенных выше формулах, но для каждого отдельно взятого предприятия формулы могут быть усовершенствованы, ввиду специфики конкретно направления бизнеса. Модель оценки потерь помогает вычислить реальные затраты на обновление и покупку нового ПО, что дает возможность избежать большинство угроз, которые могут быть характерны для сегодняшнего ПО системы.

Дополнительно следует учесть, что модель оценки потерь показывает, какие потери компания может понести, в какой срок, чтобы не разориться полностью и не выпасть из своего сегмента рынка. То есть, подвести расчет, показывающие максимально возможные потери, после которых компания может продолжать работу, а где потери, которые являются критичными и следует идти на крайние меры, чтобы не войти в дополнительные убытки.

Выводы

Как показывает анализ, для оптимизации затрат на защиту, минимизацию финансирования и получения наилучшего результата целесообразно разработать модель оценки потерь.

К преимуществам использования данной модели оценки потерь следует отнести: простота расчета, все показатели, используемые в формулах, являются открытыми данными, наглядность, то есть конкретные показатели потерь дают возможность реальной оценки понятия «потерянный доход»; легкое обучение пользователей методике работы с моделью; возможность использования на любом, даже мелком, предприятии; мониторинг системы защиты от изменений жизненно важной информации и создание плана максимально быстрого ее восстановления.

К недостаткам модели следует отнести: нет возможности прогнозирования новых потенциальных угроз; не учитывается возможная инфляция; субъективность оценки значимости информации.

Проведя анализ модели оценки потерь, можно сделать вывод, что, не смотря на то, что модель является составной частью системы информационной безопасности предприятия, ей следует уделять максимум внимания. Благодаря этой модели владельцы и собственники предприятий могут реально оценить ситуацию с бизнесом и выделить достаточно средств для соответствия уровню безопасности выдвигаемым требованиям – обеспечению заданных параметров конфиденциальности, целостности и доступности информации.

Для этого требуется: предоставлять минимальный доступ сотрудников к тем программам и функциям, которые необходимы для выполнения их рабочих обязанностей; проводить тренинги сотрудников по повышению квалификации с целью уменьшения количества непреднамеренных ошибок; наличие мотивации финансирования у владельцев для предоставления высокого уровня защиты наиболее уязвимых узлов системы; своевременно обновлять информационные узлы системы.

Литература

1. IT-портал CITForum. [Electronic resourse] / Интернет-ресурс. – Режим доступа: http://citforum.ru/security/articles/threats/ – Как определить источники угроз? Сергей Вихорев, Роман Кобцев. Открытые системы No.7-8/2002.

2. 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.

3. Защита информации и Информационная безопасность [Electronic resourse] / Интернет-ресурс. – Режим доступа: www/ URL: http://www.zashita-informacii.ru/ – Угроза доступности. Угроза конфиденциальности.