УДК 658.29-049.5

АКТУАЛЬНЫЕ ВОПРОСЫ РЕЙТИНГОВЫХ ОЦЕНОК ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.В. МАЛИКОВ, И.В. БЕНЕДИКТОВИЧ, С.А. ЧУРЮКАНОВ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
malvvv104@mail.ru

Предложен подход для рейтинговых оценок инцидентов информационной безопасности, основанный на комплексной оценке инцидента по критерию близости совокупного (реального и потенциального) ущерба с учетом уровня технологичности атак.

Ключевые слова: рейтинговые оценки инцидентов информационной безопасности, совокупный ущерб, уровень технологичности атак, оптимизация рисков.

В настоящее время наблюдается значительный количественный и качественный рост числа инцидентов информационной безопасности на объектах различных категорий [1]. Основная часть таких инцидентов осуществляется удаленно через каналы сопряжения и коммуникации. В связи с тем, что владельцами каналов, как правило, являются организации связи, необходима разработка дополнительных нормативно-правовых, организационно-технических и технических мер по их защите.

Одним из эффективных способов, позволяющих охарактеризовать риск произошедшей атаки и сформировать предположения по тенденциям ее дальнейшего развития является создание рейтинговых оценок инцидентов информационной безопасности.

В качестве определяющих параметров оценки множества инцидентов информационной безопасности предлагаются следующие:

1. Совокупный (финансовый и не финансовый) ущерб – $S_{сов.}$
2. Относительный уровень возмещения ущерба – $К_{отн}$.

В качестве дополнительного параметра оценки множества инцидентов информационной безопасности предлагается - параметр технологичности инцидента – $К_{техн}$.

Таким образом, на основе изложенного выше, представление рейтинговой оценки инцидента на основе уровневой значимости инцидентов информационной безопасности – $У_{инц}$ с учетом описанных параметров оценки будет иметь вид:

$$У_{инц}=\{S_{сов}, К_{отн}, К_{техн}\}. \quad (1)$$

Для экономической оценки совокупного (финансового и нефинансового) ущерба инцидента информационной безопасности объекта $S_{сов}$ – предлагается проведение анализа по двум направлениям:

1. Реальный ущерб – ущерб, обладающий признаками: последствия очевидны и документируемы; возможно проведение конечного экономического расчета суммы ущерба.

2. Потенциальный ущерб – ущерб, обладающий признаками: последствия не всегда очевидны и явно документируемы; возможно проведение ориентировочного (предполагаемого) экономического расчета суммы ущерба.

Оценку величины совокупного (финансового и не финансового) ущерба $S_{сов}$ – с отнесением к одному из уровней значимости предлагается осуществлять по двум параметрам:

1. Пороговая величина ущерба, определяемая нормативно-правовыми актами.

2. Относительный уровень возмещения ущерба $К_{отн}$ – определяемый величиной совокупного ущерба – $S_{сов}$ по отношению к совокупной стоимости компании (ресурсов компании) – $S_{ст}$.

В качестве дополнительного показателя оценки инцидента информационной безопасности объекта предлагается ввести параметр технологичности инцидента – $К_{техн}$, показатели которого будет иметь следующие возможные значения:

1. Высокотехнологичный инцидент (H): инцидент не описан в базах знаний по уязвимостям; инцидент является результатом таргетированной атаки (0-day, Watering Hole, социальная инженерия) [2].

2. Низко технологичный инцидент (L): инцидент полностью описан в базах знаний по уязвимостям и сборниках эксплойтов; инцидент не является результатом таргетированной атаки.

3. Смешанный инцидент (HL): инцидент частично описан в базах знаний по уязвимостям и сборниках эксплойтов; инцидент является результатом таргетированной атаки.

В качестве базовых уровней значимости инцидента информационной безопасности – $У_{инц}$ по критерию близости совокупного (реального и потенциального) ущерба предлагаются уровни: A, B, C, D (табл. 1).

Табл. 1. Базовые уровни значимости инцидента информационной безопасности

<table>
<tr><td rowspan="2">$У_{инц}$</td><td colspan="5">Пороговая величина совокупного ущерба по НПА</td><td rowspan="2">$К_{отн}$</td></tr>
<tr><td>Особо крупный</td><td>Крупный</td><td>Значительный</td><td>Средний</td><td>Мелкий</td></tr>
<tr><td>A</td><td>AAA</td><td>AA</td><td colspan="3" rowspan="2">-</td><td>$К_{отн} > 0,5$</td></tr>
<tr><td>B</td><td>BBB</td><td>BB</td><td>$К_{отн} \leq 0,5$</td></tr>
<tr><td>C</td><td colspan="2" rowspan="2">-</td><td>CCC</td><td>CC</td><td>C</td><td>$К_{отн} > 0,5$</td></tr>
<tr><td>D</td><td>DDD</td><td>DD</td><td>D</td><td>$К_{отн} \leq 0,5$</td></tr>
</table>

Таким образом, предложенный выше подход для рейтинговых оценок инцидентов информационной безопасности, основанный на комплексной оценке инцидента по критерию близости совокупного (реального и потенциального) ущерба с учетом уровня технологичности атак, позволяет провести эффективную оценку совокупного ущерба, возможности дальнейшего функционирования объекта и проведения компенсационных выплат по результатам инцидента. Практическое использование рейтинговых оценок инцидентов информационной безопасности со стороны владельцев каналов сопряжения и коммуникаций позволит оптимизировать риски для финансово-экономической деятельности объектов связи.

Список литературы

1. DDoS-атаки первого полугодия 2013 года // securelist.com [Электронный. ресурс]. – 2013. – Режим доступа: http://www.securelist.com/ru/analysis/208050810/DDoS_ataki_pervogo_polugodiya_ 2013_ goda – Дата доступа: 10.01.2014.

2. Политики безопасности: нецелевое использование ресурсов // securelist.com [Электронный ресурс]. – 2013. – Режим доступа: http://www.securelist.com/ru/blog/20776 8878/ Politiki_bezopasnosti_netselevoe_ ispolzovanie_resursov – Дата доступа: 10.01.2014.