МЕТОДИКА ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

Е.Н. Надеждин, В.А. Шептуховский
Россия, г. Москва

Характерной особенностью современного этапа информатизации отечественного образования является активное формирование распределенной инфраструктуры образовательных учреждений (ОУ) [1]. Наибольшее развитие получили сети с клиент-серверной архитектурой. Изучение статистики компьютерных преступлений показало, что наряду с расширением спектра и повышением качества сервисных услуг в образовательных сетях существенно обострилась проблема обеспечения информационной безопасности (ИБ). В настоящее время вопросы защиты информации и управления ИБ в корпоративных вычислительных сетях (КВС) преимущественно решаются штатными сотрудниками службы сетевой безопасности, располагающей определенным административным и технологическим ресурсами [2, 3].

В докладе обоснованы назначение и компонентный состав автоматизированного рабочего места (АРМ) системного администратора информационной безопасности (организации). На основе анализа функционала деятельности системного администратора выделена и сформулирована задача анализа информационных рисков. Предложено анализ информационных рисков осуществлять на основе методики, поддерживающей автоматизированное решение следующих информационно-взаимосвязанных задач:

а) идентификация информационных активов ОУ;

б) определение ценности идентифицированных активов;

в) мониторинг состояния ресурсов, идентификация существующих угроз и уязвимостей для идентифицированных активов; г) прогностическая оценка

рисков (ущерба) в случае реализации существующих угроз.

Важным этапом анализа рисков является выявление источников основных угроз распределенным ресурсам информационной образовательной среды. Опираясь на известные работы в этой области, авторы предложили вероятностные модели различных типов злоумышленников, характерных для ОУ (студент, штатный сотрудник, хакер-одиночка, хакерская группа, фирма-конкурент), отличающихся по своим целям, мотивам и используемым средствам. С использованием инструментария CASE-технологий рассмотрены функциональные модели информационных потоков, позволяющие выявить основные виды уязвимостей для защищаемых информационных активов вуза. Приведена типизация основных видов ущерба, которые может понести ОУ от реализации возможных угроз в КВС. В интересах вероятностной оценки информационных рисков применена технология когнитивного моделирования, получившая развитие в последние годы [2]. Наши исследования направлены на создание специального программного обеспечения АРМ системного администратора, осуществляющего автоматизированное ситуационное управление рисками информационной безопасности в КВС ОУ.

Предложены алгоритмы оценки защищенности информационных активов вуза, основанные на построении и анализе нечетких когнитивных карт. Когнитивная карта рассматривается как знаковый ориентированный граф, в вершинах которого располагаются ключевые факторы объекта моделирования (концепты), связанные между собой дугами, отображающими причинно-следственные связи между ними. Эти связи характеризуют степень (силу) влияния концептов друг на друга и задаются с помощью нечетких весов $Q = \{q_{ij},\, i = \overline{1,m},\; j = \overline{1,n}\}$, интервальных оценок или лингвистических термов. В общем случае, нечеткая когнитивная карта определяется как кортеж множеств: $K = (S, F, Q)$, где S – конечное множество вершин (концептов); F – конечное множество связей между концептами; Q – конечное множество весов этих связей.

Суммарный риск G по отношению к рассматриваемому множеству угроз с использованием когнитивных карт определяется выражением:

$$G = \sum_{i=1}^{m} \sum_{j=1}^{n} w_j \cdot G_{ij} ,$$

где m - количество существенных угроз; n - количество целевых факторов; w_j - значимость j-го целевого фактора, определяемая эвристически.

Риск j-го целевого фактора по отношению к i-й угрозе G_{ij} вычисляют на основе соотношения: $G_{ij} = P_i \cdot H(S_i^V \to S_j^D) \cdot f_j$. Здесь P_i - вероятность i- угрозы; $H(S_i^V \to S_j^D)$ - приведенный эффект воздействия угрозы S_i^V на целевой фактор S_j^D, f_j - показатель, отражающий ценность j -го ресурса.

Задавая стоимость целевых факторов S_j^D, по предложенной методике можно определить потенциальный риск (ущерб) как для отдельных целевых факторов от действия тех или иных угроз, так и общий (суммарный) риск. Использование технологии когнитивного моделирования позволяет не только выявлять негативные процессы в КВС при действии одиночных и групповых угроз, но и указать потенциально уязвимые места в системе защиты и пути компенсации (или ослабления) воздействия угроз за счет выбора оптимальных механизмов защиты информации и информационных ресурсов.

Применение разработанных рекомендаций позволяет замкнуть контур управления рисками информационной безопасности, добиться снижения уровня информационных рисков до приемлемых значений, отвечающих нормативным требованиям политики корпоративной безопасности.

Литература

1. Надеждин Е.Н. Научно-методические основы автоматизации процессов обеспечения информационной безопасности в сфере образования // Ученые

записки ИИО РАО. 2012. № 41. С.56-74.

2. Васильев В.И., Кудрявцева Р.Т. Анализ и управление информационной безопасностью вуза на основе когнитивного моделирования // Системы управления и информационные технологии. 2007. № 1(27). С. 74-81.

3. Надеждин Е.Н., Малышев В.А., Шептуховский В.А. К вопросу обеспечения информационной безопасности ресурсов корпоративных сетей науки и образования / Надеждин Е.Н., Малышев В.А., Шептуховский В.А.; ИИО РАО. – г. Москва, 2010. – 14 с. Библиогр.: 14 назв. – Русс. – Деп. ВИНИТИ 24.02.2011 г. № 80-В2011.