УДК 004

Николаева А.Н.,
Студент
4 курс, Отделение геологии
Национальный исследовательский Томский политехнический университет
Россия, г. Томск

АНАЛИЗ И МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ РИСКОВ ГЕОКОМПАНИИ

Аннотация: *Проблеме прогнозирования (моделирования, аудита) ИКТ-рисков в геоинформационных системах отводится мало ресурсов (времени, внимания, обеспечения). Но это основа политики безопасности нефтегазодобывающей организации. Важно иметь не только политику безопасности, но и модели («портреты») нарушителей, сценарии проникновения их в системы. Работа посвящена этой проблеме.*

Ключевые слова: *моделирование, риски, информационные, прогнозирование, геокомпания, система.*

Annotation: *The problem of forecasting (modeling, auditing) of ICT risks in geographic information systems is allocated little resources (time, attention, support). But this is the basis of the security policy of the oil and gas producing organization. It is important to have not only a security policy, but also models ("portraits") of violators, scenarios of their penetration into systems. The work is devoted to this problem.*

Keywords: *modeling, risks, information, forecasting, geocompany, system.*

Аналитика, прогнозирование (моделирование) информационных, ИКТ-рисков, их аудит – важнейшая проблема подсистемы безопасности, построения релевантной политики безопасности нефтегазодобывающей компании,

организации. Но политика безопасности, минимизации информационных рисков геокомпании строится на реальных моделях нарушителей, сценариях проникновения их в сети, геоинформационные системы (ГИС).

Универсальных моделей нарушителей (нарушений) нет, каждая адаптируется на конкретную ГИС, конкретный защищаемый объект, процесс.

Моделирование нарушений, нарушителей. Любая модель – отражение реальности, абстракции, описание (представление) одной системы языком, средствами другой системы [1]. В модели нарушителя отражаются цели, мотивации, гипотезы поведения, компетенции, инструментарий противоправных действий, приводящих к финансовому, материальному, технологическому, имиджевому ущербу атакуемой стороны. Немаловажно учитывать и социально-экономическую, гуманитарную категорию, группу, к которой принадлежит данный нарушитель.

В свою очередь, это определяет возможности нарушителя, группы, например, операционные, информационно-технологические. Аналогично существующей, достаточно полной, четкой классификации опасностей для ГИС, необходимо классифицировать и потенциальные действия, и потенциальный ущерб от нарушителя. Здесь возможны различные методы классификации, например, 10-уровневая система шкалирования.

Можно определить матрицу R степеней риска для различных категорий пользователей

$$R\ ||r_{ij}\ ||, i = 1,2, \dots, m;\ j = 1,2, \dots, n\ .$$

Строки отождествляются с категориями пользователей: руководитель отдела, администратор безопасности, системный программист, пользователь, прикладной программист, администратор БД и др. Столбцы – с факторами, точками риска в ГИС: потеря информации, снижение производительности, временная недоступность, блокирование риска и др.

Элементы r_{ij} – с оценками в баллах (или относительных величинах) степени риска для профессионально выполняемых функций i-ой категорией

пользователей при j-ых рисках. Например, если $r_{ij} = 8$, то руководитель подразделения может недополучать 80% необходимой информации.

Потенциальный сценарий поведения нарушителя, его модель конкретизируется, возможно, модифицируется.

Наряду с матрицей R рисков рассмотрим матрицу Q, характеризующую каждую группу вероятных нарушителей

$$Q = || \ q_{jk}||, i = 1,2, \dots, m; k = 1,2, \dots, K \ ,$$

где q_{ik} – k-ый параметр i-ой группы. Например, техническая оснащенность нарушителя, «точки входа» нарушителя, длительность (промежуток) воздействия и др. В частности, техническая оснащенность (инструментарий) взломщика может включать средства [2]:

1) пассивные (без вмешательства в архитектуру, без модификации, использующие лишь уязвимость системы);

2) активные (с вмешательством, изменением архитектуры, регламента взаимодействий, специальных технических средств и программ).

Итак, если M – модель атаки на ГИС, то ее можно описать кортежем вида

$$M \ = < K, N, V, T, Q, P, U, >,$$

где K– класс опасности воздействия, N – класс (тип) нарушителя, V – места воздействия («точки входа»), T– время (период совершения нарушения), Q – время обнаружения атаки, P – вероятности атаки, U – возможные ущербы атаки.

Идентифицируется профиль атаки, суживается область поиска, сокращается время реагирования, совершенствуется политика безопасности. Хотя многие факторы, процессы, учитываемые моделью M – качественного типа, существуют интервальные, многомерного шкалирования, статистические, нечеткие и другие способы определения количественных характеристик, верификации атаки нарушителя.

Современные методики анализа, прогноза рисков, построения и выполнения политики безопасности ориентированы на количественную аналитику [3], оценку риск-состояний, оценку затрат на блокирование,

«закрытие» уязвимостей в «доатакуемый» период, адаптацию к «атакуемому периоду».

Необходима методологическая, риск-аналитическая система ГИС нефтегазодобывающей компании [4].

Заключение. Классифицируем меры по уровням:

1) менеджмент высшего уровня (гендиректор, руководитель компании, организации) – выработка политики безопасности компании, согласование, обоснование, оценка состояния и критериев информационной безопасности организации и др.;

2) менеджмент среднего уровня (руководители подсистем, департаментов безопасности, филиала) – оценивание текущего состояния безопасности компании на всех этапах ее актуализации, выработка мероприятий, корпоративных критериев, норм (архитектура работ, положение о рекламе, коммерческой тайне, должностные инструкции, оценка инвестиций в подсистему безопасности, вопросы сертификации и стандартизации, например, ISO и др.);

3) менеджмент низшего звена (сетевые администраторы, системные программисты, руководители кадрового отдела) – оценка текущей объективной безопасности, сервисно-интерфейсных, информационно логических инструментов, брандмауэров, оболочек, элементов политики безопасности и др.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Казиев В.М. Введение в анализ, синтез и моделирование систем. – М.: Бином. Лаборатория знаний. Интуит.ру. –2007. -244с.

2. Шпак В.Ф. Знай противника своего // Защита информации. Конфидент, №2, 2002, с. 60-68.

3. Паклин Н., Орешков В. Бизнес-аналитика: от данных к знаниям (2-ое изд.) – СПб.: Питер, 2010, -590с.

4. Симонов С.М. Методология анализа рисков в информационных системах. Защита информации. Конфидент, №1, 2001, с. 72-76.