МЕТОДЫ ОЦЕНКИ СТЕПЕНИ СООТВЕТСТВИЯ ПОДРАЗДЕЛЕНИЙ СЛОЖНОЙ СЕТИ ПОКАЗАТЕЛЯМ КОРПОРАТИВНОЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Козлов А.Д., Нога Н.Л.

Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная д.65
alkozlov@ipu.ru, noga@ipu.ru

Аннотация. Предложены методы оценки степени соответствия подразделений сложной распределенной корпоративной информационной системы ряду показателей информационной безопасности. В результате реализации методов дается сравнительная оценка степени удовлетворения требованиям корпоративной политики информационной безопасности каждого из подразделений с целью дальнейшего принятия решений руководством корпорации относительно мер по минимизации рисков в результате возможного осуществления угроз информационной безопасности.

Ключевые слова: информационная безопасность, критерии, ранжирование значений показателей, сравнительная оценка, отношение Парето, максиминная и минимаксная процедуры, счета Борда, расстояние Хэмминга.

Введение

В последнее время одной из важнейших задач организаций, в силу развития цифровизации экономики, является защита информационных ресурсов. Основные требования по обеспечению безопасности этих ресурсов обычно формулируются в документах по корпоративной политике информационной безопасности.

В этом документе в соответствии с принятыми стандартами прописываются правила по сбору, хранению, обработке и доступу к информации, как сотрудников, так и внешних пользователей. Определяется их ответственность на всех этапах прохождения информации. А также, задаются характеристики обрабатываемой информации, формулируются различные организационные, технологические и технические требования к обеспечению информационной безопасности.

Для обеспечения защиты информационных ресурсов компания должна осуществлять постоянный мониторинг состояния информационной безопасности, фиксировать любые неправомерные попытки нарушения доступности, целостности, конфиденциальности информации. По результатам мониторинга и анализа уязвимостей и фактов нарушения, служба безопасности компании должна предлагать руководству компании решения по минимизации возможного ущерба от возникающих угроз информационной безопасности.

Для организаций (корпораций), имеющих территориально-распределенную структуру задача принятия управленческих решений существенно усложняется, так как одновременно охватить все подразделения невозможно. Поэтому важно выявить наиболее критичные подразделения. Сделать это помогает их ранжирование. В работе авторов [1] рассматривался метод ранжирования подразделений, но не было дано сравнительной оценки полученных результатов с другими методами.

В настоящем докладе авторы предлагают рассмотреть методы ранжирования и сравнительной оценки подразделений по ряду важных показателей, утвержденных корпоративной политикой информационной безопасности. В результате реализации таких методов будет обеспечена сравнительная оценка степени удовлетворения требованиям информационной безопасности каждого из подразделений и найдены наиболее критичные из них для дальнейшего моделирования разнообразных управленческих ситуаций, генерации на этой основе решений по реализации мер по защите информационных ресурсов корпорации.

Постановка задачи

Вышеуказанные показатели будем в дальнейшем рассматривать как некоторые критерии, принимающие значения из определенных интервалов, стандартные границы которых определяются как в международных стандартах, так и в различных методических и нормативных документах организации. Каждому подразделению корпорации поставим в соответствие некоторый ранг r, в зависимости от значений этих критериев, и выстроим все ранги, например, по возрастанию. Будем считать, что чем выше ранг, тем выше степень удовлетворения требованиям информационной безопасности.

Пусть B – множество рассматриваемых подразделений, куда входят подразделения, обозначенные как $x, y, z,...$; I – количество рассматриваемых показателей, K_i – i-й показатель, $i = 1,\ldots,I$; $r_j = r_j(K_1, K_2, ..., K_I)$ – ранг j-го подразделения, $j = 1, \ldots, N$, где N - количество рассматриваемых

подразделений. В предположении, чем больше значение ранга, тем лучше обстоят дела с обеспечением информационной безопасности подразделения, необходимо отсортировать ранги по возрастанию.

Предположим, что мы оцениваем подразделение *x* по *i* показателям, то есть:

$$K_1(x), K_2(x), ..., K_i(x).$$

Далее проведем реализацию методики на примере из [1] (рассматривается одна из корпораций с разветвленной сетью подразделений в качестве примера) оценки 10 подразделений по 3 критериям (показателям), которые указывают степень удовлетворения требованиям информационной безопасности подразделения по каждому показателю. Для оценки выбираются следующие показатели: F – частота появления неправомерных запросов, поступивших из j-го подразделения по отношению к общему числу запросов от этого подразделения; S – частота предотвращенных инцидентов безопасности в j-м подразделении по отношению к общему числу выявленных инцидентов в данном подразделении; D – относительное количество пользователей в j-м подразделении, выполняющих требования политики безопасности по смене пользовательских паролей.

Далее предлагаются к рассмотрению несколько достаточно простых методов ранжирования подразделений, результаты сравниваются с целью выбора наиболее оптимального метода, используя расстояние Хэмминга [2]. Первые два метода основаны на игровых матрицах: метод максиминной процедуры и максимизации выигрышей, метод минимаксной процедуры и минимизации выигрышей. Третий метод основан на методе счетов Борда, четвертый - на методе усреднения счетов Борда [3].

Заключение

Задача оценки степени удовлетворения требованиям информационной безопасности каждого из подразделений территориально-распределенной организации со сложной структурой - необходимая, хотя и достаточно трудная задача, с которой приходится иметь дело службе информационной безопасности организации. В данной ситуации можно пойти разными путями. Один из путей – это предложить службе информационной безопасности определить целевую функцию по большому набору переменных, связанных с угрозами, уязвимостями и ущербом, чтобы иметь возможность управлять оказанием различных информационных услуг в зависимости от множества как экономических, так и организационных условий. При этом сотрудники этой службы должны обладать незаурядными способностями по обработке такой информации. Другой путь предложен в данном докладе. Он значительно уменьшает информационные требования к сотрудникам службы информационной безопасности организации, предлагая этой службе сформировать функцию выбора, основанную на предлагаемых выше методах ранжирования. В зависимости от задачи, поставленной руководством, например, ввести наказание за допущенные ошибки в процессе обеспечения информационной безопасности подразделений, рекомендуется использовать тот или иной метод. Как только службой информационной безопасности организации произведена оценка состояния информационной безопасности в подразделениях, можно принимать соответствующие решения, одобренные руководством организации.

Необходимо отметить, что предложенные методы можно применять к любой сложной сетевой структуре, как государственных органов, так и частных корпораций, что позволяет учитывать региональные особенности подразделений (количество и квалификацию сотрудников в подразделении, удаленность и т.п.).

Литература

1. Козлов А.Д., Нога Н.Л. Методика ранжирования подразделений распределенной корпоративной системы по степени соответствия политике информационной безопасности / Труды XIII всероссийского совещания по проблемам управления (ВСПУ-2019). М.: ИПУ РАН, 2019. (в печати)

2. Alex X. Liu, Ke Shen, Eric Torng. Large Scale Hamming Distance Query Processing. ICDE Conference, - P.553 — 564, 2011.

3. Быстров О.Ф., Поздняков В.Я., Прудников В.М., Перцов В.В., Казаков С.В. Управление инвестиционной деятельностью в регионах Российской Федерации. - М.: ИНФРА-М, 2008. – 358с.