УДК 621.391

ОЦЕНКА УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТИПОВОЙ КОРПОРАТИВНОЙ СЕТИ

А. Н. Назаров, начальник отдела ОАО «Интеллект Телеком», д.т.н., nazarov@i-tc.ru
М. М. Климанов, аспирант МФТИ

Ключевые слова: *сети связи следующего поколения (NGN), уровень информационной безопасности, Л-функция, В-полином.*

Введение. Одним из важнейших направлений научно-технического прогресса в настоящее время являются инфокоммуникационные системы, представляющие собой сети передачи и хранения информации. Наиболее перспективные подходы к построению таких сетей отражены в концепции NGN (Next Generation Networks) — сетей связи следующего поколения, преследующих цель объединения ресурсов информационных технологий и развитой инфраструктуры электросвязи для обеспечения доступа к ним любого пользователя в реальном времени. При таком объединении вопросы обеспечения необходимого уровня информационной безопасности для разных классов пользователей инфокоммуникационной сети (ИКС) приобретают особую важность.

Особую актуальность для ИКС представляют методически-законченные интегральные оценки уровня информационной безопасности. Так как ИКС, равно как и любые другие сложные системы, подвержены воздействию множества различных дестабилизирующих факторов (ДФ), то вопросы практической оценки защищенности существующих и проектируемых ИКС встают достаточно остро.

Постановка задачи. Риск некоторого объекта Y, принадлежащего ИКС и подвергающегося атаке со стороны нарушителя, состоит из двух компонент [1,2]: вероятности неуспеха противодействия атаке в отношении объекта Y (далее — неуспех объекта Y) или вероятности проведения успешной атаки и оценки (например, финансовой, материальной, временной на устранение ущерба и др.) масштаба последствий (ущерба) успешной атаки.

Объект риска считается достаточно защищенными, если с учетом возможности потенциального преодоления преград вероятность успешной атаки (риска, неуспеха объекта риска) $P_A^Y = \left(1 - P_з^Y\right)$ меньше допустимого значения $P_{A-ДОП}^Y$, т. е. условие достижимости

$$P_з^Y \geq 1 - P_{A-ДОП}^Y,$$

где $P_з^Y$ — вероятность успешного противостояния атаке (защищенность, вероятность успеха объекта риска) объектом риска.

Для произвольного объекта риска Y из ИКС [1] существует полная система (перечень) функций защиты (или признаков), каждую из которых обозначим бинарной логической переменной X с соответствующим нижним индексом:

X_1 — предупреждение возникновения условий, благоприятствующих порождению (возникновению) ДФ;

X_2 — предупреждение непосредственного проявления ДФ;

X_3 — обнаружение проявившихся ДФ;

X_4 — предупреждение воздействий на объект риска, проявившихся и обнаруженных ДФ;

X_5 — предупреждение воздействий на объект риска, проявившихся, но необнаруженных ДФ;

X_6 — обнаружение воздействия ДФ на объект риска;

X_7 — локализация (ограничение) обнаруженного воздействия ДФ на объект риска;

X_8 — локализация необнаруженного воздействия ДФ на объект риска;

X_9 — ликвидация последствий локализованного обнаруженного воздействия ДФ на объект риска;

X_{10} — ликвидация последствий локализованного необнаруженного воздействия ДФ на объект риска.

Результат выполнения каждой из функций защиты или ее исход является случайным событием и может принимать два значения — успех или неуспех. Следуя логике [1], положим, что бинарная логическая переменная $X_j, j = 1 \div n, n = 10$, равна 1 с вероятностью P_j, если выполнение j-й функции защиты привело к неуспеху объекта риска, и равна 0 с вероятностью $Q_j = 1 - P_j$ — в противном случае.

Преграды, создаваемые для противодействия негативным воздействиям ДФ на объект риска, выполняют определенные функции защиты, препятствующие осуществлению атаки на объект риска со стороны злоумышленника. При этом одна преграда может выполнять последовательно несколько функций защиты или одну функцию защиты по отношению к разным объектам риска.

В общем виде логическая функция (Л-функция) неуспеха объекта риска [1] записывается как

$$Y = Y(X_1, ..., X_n),$$

а вероятностная функция (В-функция, В-полином) неуспеха

$$P(Y = 1/X_1, ..., X_n) = \Psi(P_1, ..., P_n) = PY.$$

Вывод Л-функции

$$\begin{aligned} Y = {} & X_1X_2\left(\overline{X_3}X_4 \vee X_3X_5\right)\overline{X_6X_7}X_9 \vee \\ \vee {} & X_1X_2\left(\overline{X_3}X_4 \vee X_3X_5\right)X_6\overline{X_8}X_{10} \vee X_1X_2\left(\overline{X_3}X_4 \vee X_3X_5\right)\overline{X_6}X_7 \vee \\ \vee {} & X_1X_2\left(\overline{X_3}X_4 \vee X_3X_5\right)X_6X_8 \end{aligned} \quad (1)$$

для общего случая приводится в [1].

На основе (1), применяя рекомендации [1, 3, 4], получим выражение для В-полинома:

$$\begin{aligned} PY = PY(P_1, P_2, \ldots, P_{10}) = {} & P_1P_2\left[\left(1 - P_3\right)P_4 + P_3P_5\right] \times \\ \times {} & \left[\left(1 - P_6\right)\left(1 - P_7\right)P_9 + P_6\left(1 - P_8\right)P_{10} + \left(1 - P_6\right)P_7 + P_6P_8\right]. \end{aligned} \quad (2)$$

Формула (2) позволяет получить численное значение вероятности незащищенности (неуспеха) объекта риска Y при проведении в отношении него атаки злоумышленником.

Классификация значений вероятности незащищенности по различным категориям приведена в табл. 1 [5].

Анализируя табл. 1 и выражения (1), (2), можно сделать вывод о необходимости дальнейших исследований в направлении оценивания парциального влияния (важности, значимости) функций защиты $X_j, j = 1 \div n, n = 10$, на Л-функцию (1) и значений вероятностей P_j и Q_j на В-полином (2) объекта риска Y.

Таблица 1

Категория риска	Значение вероятности незащищенности PY объекта риска
Незначительные	$PY \le 0{,}300$
Существенные	$0{,}301 \le PY \le 0{,}599$
Критические	$0{,}600 \le PY \le 0{,}999$

Оценка парциального влияния функций защиты на интегральную оценку защищенности объекта риска. Определим веса или парциальное влияние каждого из 10 элементов, входящих в уравнение (2), с помощью формулы, представленной в [4]:

$$g_{x_i} = \sum_{f=1}^{k} 2^{-(r_f - 1)} - \sum_{j=1}^{l} 2^{-(r_j - 1)}, \qquad (3)$$

где k, r_f — число и ранг (количество различных аргументов) ортогональных конъюнкций, содержащих аргумент X_i в Л-функции (1); l, r_j — число и ранг ортогональных конъюнкций, содержащих аргумент $\bar{X}_i$ в той же Л-функции (1). Заполним значениями весов табл. 2.

Таблица 2

Аргументы $X_j, j = 1 \div n, n = 10$	Значения весов g_{xi}
X_1	0,1875
X_2	0,1875
X_3	0
X_4	0,09375
X_5	0,09375
X_6	0
X_7	0,03125
X_8	0,03125
X_9	0,03125
X_{10}	0,03125

Выясним, какая из функций защиты вносит наибольший вклад в защищенность объекта риска. Для этого необходимо установить коэффициенты чувствительности функции PY ко вкладу каждой из функций защиты в рассматриваемых точках. Под коэффициентом чувствительности функции PY к какой-либо функции защиты в некоторой точке многомерного вероятностного пространства будем понимать отношение изменения значения функции PY к бесконечно малому изменению вероятности успеха соответствующей функции защиты, вызвавшему изменение значения PY.

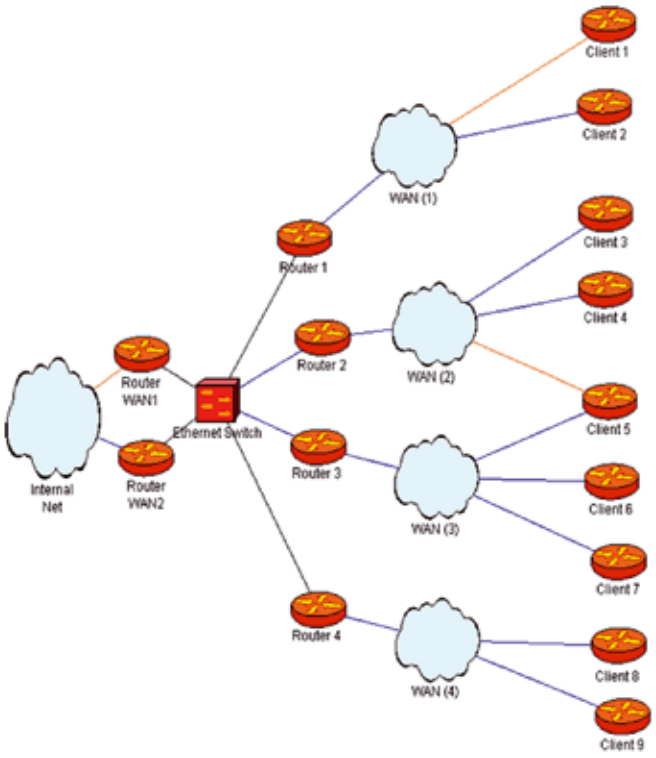
В предположении, что функция PY дифференцируема во всех точках, где определены значения P_i, $i = 1 \div 10$, коэффициентом чувствительности будет $\dfrac{\partial PY}{\partial P_i} = \xi_i$ — первая частная производная функции PY по соответствующей P_i, $i = 1 \div 10$. Распишем все коэффициенты чувствительности в общем виде:

$$\begin{cases}
\xi_1 = P_2\left[(1-P_3)P_4 + P_3P_5\right]\left[(1-P_6)(1-P_7)P_9 + (1-P_6)P_7 + P_6(1-P_8)P_{10} + P_6P_8\right];\\
\xi_2 = P_1\left[(1-P_3)P_4 + P_3P_5\right]\left[(1-P_6)(1-P_7)P_9 + (1-P_6)P_7 + P_6(1-P_8)P_{10} + P_6P_8\right];\\
\xi_3 = P_1P_2(P_5 - P_4)\left[(1-P_6)(1-P_7)P_9 + (1-P_6)P_7 + P_6(1-P_8)P_{10} + P_6P_8\right];\\
\xi_4 = P_1P_2\left[1-P_3\right]\left[(1-P_6)(1-P_7)P_9 + (1-P_6)P_7 + P_6(1-P_8)P_{10} + P_6P_8\right];
\end{cases}$$

↓

$$\begin{cases}
\xi_5 = P_1P_2P_3\left[(1-P_6)(1-P_7)P_9 + (1-P_6)P_7 + P_6(1-P_8)P_{10} + P_6P_8\right];\\
\xi_6 = P_1P_2\left[(1-P_3)P_4 + P_3P_5\right]\left[(P_7-1)P_9 + (1-P_8)P_{10} - P_7 + P_8\right];\\
\xi_7 = P_1P_2\left[(1-P_3)P_4 + P_3P_5\right]\left[(P_6-1)P_9 + (1-P_6)\right];\\
\xi_8 = P_1P_2\left[(1-P_3)P_4 + P_3P_5\right]\left[P_6(1-P_{10})\right];\\
\xi_9 = P_1P_2\left[(1-P_3)P_4 + P_3P_5\right]\left[(1-P_6)(1-P_7)\right];\\
\xi_{10} = P_1P_2\left[(1-P_3)P_4 + P_3P_5\right]\left[P_6(1-P_8)\right].
\end{cases}$$

Практический пример оценки защищенности объекта риска. Попробуем на практике рассчитать численное значение вероятности незащищенности граничного маршрутизатора, выступающего в качестве объекта риска, при проведении в отношении него атаки, направленной на изменение его таблицы маршрутизации. Упрощенная схема сети представлена на рисунке.



Маршрутизаторы клиентов (Client 1 — Client 9) сообщают граничным маршрутизаторам (Router 1 — Router 4) информацию о сетях клиентов с помощью примитивного протокола динамической маршрутизации RIPv2, что обусловлено аппаратными ограничениями клиентского оборудования. Маршрутизаторы клиентов хотя и принадлежат компаниям клиентов, но находятся под управлением специалистов организации.

Управление специалистами сетевого отдела клиентскими маршрутизаторами снижает риск отправки клиентскими сетевыми устройствами ошибочной маршрутной информации, однако не может исключить вероятность подмены роутеров клиентами. Проведение конфигурирования клиентского оборудования специалистами организации можно отнести к предупреждению возникновения условий, благоприятствующих возникновению ДФ, т. е. X_1. Успешность проведенных мероприятий можно оценить с помощью автоматического обхода всех клиентских устройств и подсчета неправильно настроенных.

Произведенная проверка 97 клиентских маршрутизаторов, подключенных к одному из роутеров (условно Router 1), на трех из которых отсутствовала типовая конфигурация, показала, что вероятность неуспеха предупреждения возникновения условий, благоприятных для проявления ДФ, можно оценить с помощью формулы $P_1 = 3/97$. Статистически это соответствует 3 % неуспеха из серии соответствующих атак.

Так как регламентом работы сетевого отдела не предусмотрено выполнения каких-либо действий по предупреждению проявления самих ДФ, то вероятность неуспеха данной функции защиты априори считается равной единице, т. е. $P_2 = 1$. Обнаружение проявившихся ДФ возможно лишь через обнаружение воздействия ДФ на объект риска, поэтому $P_3 = 1$, т. е. $Q_2 = 0$. Поскольку мероприятия, направленные на предупреждение воздействия на объект риска проявившихся и обнаруженных, либо проявившихся и необнаруженных ДФ, не проводятся, считаем вероятность их неуспеха равной единице, т. е. $P_4 = P_5 = 1$.

Обнаружить воздействие ДФ в автоматическом режиме возможно лишь для тех компаний, для которых проводится мониторинг состояния их каналов связи. Обычно это очень крупные клиенты, имеющие более одного физического канала связи. Сегодня число таких компаний составляет 15, а общее число клиентов — около 350 организаций.

Исходя из вышеизложенного, вероятность неуспеха автоматического обнаружения воздействия ДФ можно оценить по формуле

$$P_6 = \frac{350 - 15}{350} \approx 0{,}96,$$

что статистически соответствует 96 % неуспеха из серии соответствующих атак. Отсюда $Q_6 \approx 0{,}4$.

Поскольку клиенты «приводятся» на несколько маршрутизаторов сети организации, то воздействие атаки, направленной на «отравление» таблицы маршрутизации, ограничено именно тем устройством, к которому подключен данный клиент. Это обусловлено статическими картами трансляций маршрутных обновлений между различными протоколами динамической маршрутизации. Таким образом, локализуется как обнаруженное, так и необнаруженное воздействие.

Полагая, что клиенты равномерно распределены между шестью граничными маршрутизаторами, получаем, что «отравив» один маршрутизатор, можно воздействовать приблизительно лишь на 58 организаций, т. е.

$$P_7 = P_8 = \frac{\frac{350}{6} - 1}{350} = \frac{86}{525} \approx 0{,}16,$$

что статистически соответствует 16 % неуспеха из серии соответствующих атак. Тогда $Q_7 \approx Q_8 \approx 0{,}84$. В связи с тем, что возникновение ДФ гарантировано приводит к неуспеху объекта, полагаем $P_9 = P_{10} = 1$. Подставляя полученные значения вероятностей в (2), получим $PY \approx 0{,}03$. Согласно градациям из табл. 1, вероятность неуспеха защищаемого объекта относится к диапазону незначительных рисков.

Дальнейшее исследование коэффициентов чувствительности на экстремум позволит сделать вывод о том, что для улучшения полученной оценки вероятности неуспеха объекта защиты необходимо в первую очередь позаботиться о предупреждении возникновения условий, благоприятствующих порождению (возникновению) дестабилизирующих факторов.

ЛИТЕРАТУРА

1. **Назаров А. Н.** Оценка уровня информационной безопасности современных инфокоммуникационных сетей на основе логико-вероятностного подхода//АиТ. — 2007. — № 7. — С. 52—63.
2. **Денисова Т. Б.** Надежность и безопасность услуги VPN//Электросвязь. — 2005. — № 9. — С. 20—22.
3. **Ryabinin I. A.** Reliability of Engineering Systems. Principles and Analysis. — M.: Mir, 1976.
4. **Рябинин И. А.** Надежность и безопасность структурно-сложных систем. — СПб.: Изд-во С.-Петерб. Ун-та, 2007. — 276 с.
5. **Копорулин Ю. А.** Подход к количественной оценке безопасности сетей электросвязи, входящих в ССОП/Доклад на 6-й междунар. конф. «Безопасность и доверие при использовании инфокоммуникационных сетей и систем». 5—6 апреля 2007 г. — 4 с.

Получено после доработки 02.07.09