УДК 004.056
ББК 32.841

Р. А. Файрузов

Методика оценки организационных рисков при проведении социотехнического тестирования компании

Национальный Ядерный Исследовательский Университет МИФИ
г. Москва

***Аннотация**: В статье, рассмотрена проблема осведомлённости сотрудников компании в сфере информационной безопасности. Разработана методика оценки уровня осведомлённости персонала в области информационной безопасности для своевременного выявления пробелов в этой области и планирования мероприятия по повышению уровня осведомлённости сотрудников.*

***Ключевые слова**: Информационная безопасность, осведомлённость в компании, методики по оценки уровня осведомлённости в сфере информационной безопасности, организационные риски.*

Введение

На сегодня технический прогресс продвинулся далеко вперёд. Организации, заинтересованные в обеспечении информационной безопасности, зачастую стараются обойтись техническими, программными и организационными мерами, забывая про самое слабое звено, которым всегда были и являются люди, а именно персонал компании.

Одним из наиболее распространённых и эффективных способов получения несанкционированного доступа к корпоративным информационным системам извне являются атаки, основанные на взаимодействии злоумышленника с сотрудниками компании — социальная инженерия [3, 6]. На первом этапе такой атаки злоумышленник, как правило, тем или иным способом (по электронной почте, социальной сети, телефону и т. п.) связывается с сотрудником и побуждает его раскрыть какую—либо конфиденциальную информацию или может воспользоваться уязвимым приложением, чтобы просмотреть переданные сотрудником данные. Если сотрудники компании недостаточно осведомлены в области информационной безопасности, то даже при хорошей технической защите периметра сети, злоумышленник может получить доступ к сетевым ресурсам и конфиденциальной информации, например, посредством фишинга.

Возрастает процентная доля целевых фишинговых атак, организованных путём распространения писем по электронной почте, в которых можно выделить определённую организацию или группу лиц [4, 5]. Целевые пользователи получают тщательно разработанные фишинговые сообщения, заставляющие человека ввести более конфиденциальные персональные сведения, такие как логин и пароль, которые предоставляют доступ к корпоративным сетям или базам данных с важной информацией. Помимо запроса учётных данных, целевые фишинговые письма могут также содержать вредоносное программное обеспечение.

Кроме того, злоумышленник может разработать атаку и получить несанкционированный доступ к критически важным бизнес—ресурсам компании.

Такие атаки, в случае успеха, могут привести к реализации таких рисков, как потерянная прибыль из—за вмешательства в бизнес—процессы (включая различные мошеннические действия от имени скомпрометированных сотрудников), потеря конкурентных преимуществ из—за утечки конфиденциальной информации, судебные разбирательства с партнёрами и клиентами и другим репутационным, финансовым и операционным рискам [1].

В целях снижения вышеуказанных рисков следует оценивать уровень осведомлённости персонала компании в области информационной безопасности, который позволит своевременно выявить пробелы в этой области и планировать мероприятия по повышению уровня осведомлённости сотрудников.

Оценка уровня осведомлённости персонала представляет собой процесс получения несанкционированного доступа к рабочим станциям сотрудников или получения конфиденциальной информации (такой, как пароли) с помощью социальной инженерии из Интернета.

Методика оценки организационных рисков при проведении социотехнического тестирования компании

В основе методики оценки организационных рисков, направленных на анализ социальной сети компании, лежит математический аппарат (анализа социальных сетей), основанный на применении теории графов, а также метода оценки рисков. С помощью этого подхода работники компании (или отдельные подразделения) изображены вершинами социального графа, как показано на рисунке 4, а их отношения или ситуации взаимодействия — рёбрами этого графа. Особый интерес представляет совместный анализ нескольких отношений (при условии построения нескольких графов—сетей на одном множестве вершин).

При использовании устройство для анализа социальных сетей возможно обнаружить скрытых неформальных групп в компании — кластеры сотрудников (заданные подграфами полного графа) и проанализировать взаимосвязи между ними. Результаты этого анализа могут выявить индикаторы проблемного взаимодействия и обосновать корректирующие организационные мероприятия.

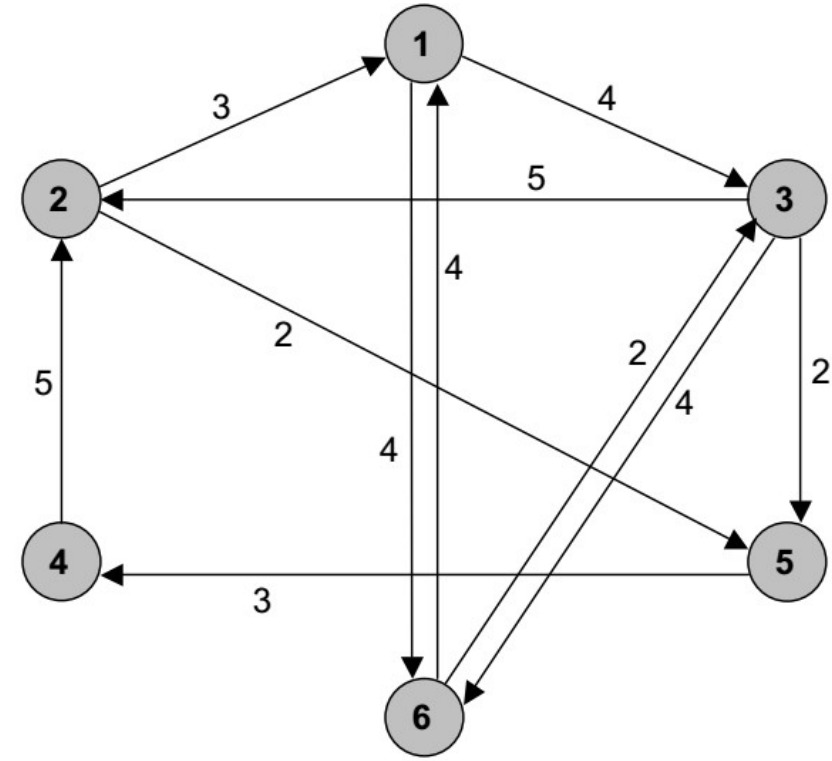


Рисунок 4 – Сильно связанный орграф с расставленными весами рёбер

Анализируя графы возможен моделирующий подход, в коим веса отдельных связей можно варьировать, добавлять и удалять новые связи, новые вершины, а также, экспериментально изменять атрибуты вершин, чтобы найти конфигурацию сети, которая наилучшим образом соответствует потребностям организации.

Сегодня существует ряд подходов к измерению рисков. В простейшем случае оценивается два фактора: вероятность происшествия и серьёзность возможных последствий. Как правило, считается, что чем больше риск, тем больше вероятность происшествия и серьёзность последствий. Итоговая концепция представляется следующей формулой:

$$R = P \times W, \text{ где} \qquad (6)$$

R – уровень риска; W – серьёзность последствий; P – вероятность происшествия.

Если переменные являются количественными величинами, то риск представляет собой оценку математического ожидания потерь. Когда переменные являются

качественные величинами, операция метрического умножения не определена. Таким образом, эту формулу нельзя использовать в явном виде [2].

В данной работе формула (6) является основой для создания методики оценки организационных рисков. Вероятность происшествия, которая в этом подходе может быть объективной или субъективной величиной, зависит от «уровня компрометации», «уровень влияния связей». Соответственно, оценка риска является результатом сочетания всех трёх показателей. Условно оценку риска можно выразить формулой:

$$R = W * P_i * P_T, \text{ где} \quad (7)$$

R – уровень риска;
W – уровень ущерба;
ρT – уровень влияния связей;
ρi – уровень компрометации.

Однако для более детального расчёта организационных рисков используем общую формулу Байеса (8). Математически теорема Байеса показывает связь между вероятностью события A и вероятностью события B, P(A) и P(B), условной вероятность возникновения события A при существующем B и возникновении события B при существующем A, P(A | B) and P(B | A).

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)}, \text{ где} \quad (8)$$

$P(A|B)$ – условная вероятность наступления события A при существующем B;
$P(B|A)$ – условная вероятность наступления события B при существующем A;
$P(A)$ – вероятностью события A, $P(B)$ – вероятностью события B.

Таким образом, общая формула Байеса позволяет учесть влияние смежных вершин (уровень влияния связи) на выбранную вершину графа.

$$R = W * \left(\frac{1}{Kn}\right) * \sum_{i=1}^{n} P_T^{'} P_i^{'} k_i, \text{ где} \quad (9)$$

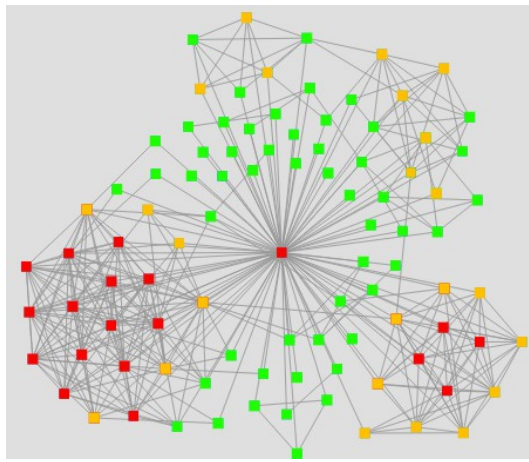
R – уровень риска;
W – уровень ущерба;
P_T – уровень уязвимости смежной вершины;
$P_i^{'}$ – уровень компрометации смежной вершины,
k – коэффициент приоритета (влияние смежных вершин на выбранную вершину графа),

Kn – уровень «знаний ИБ»,

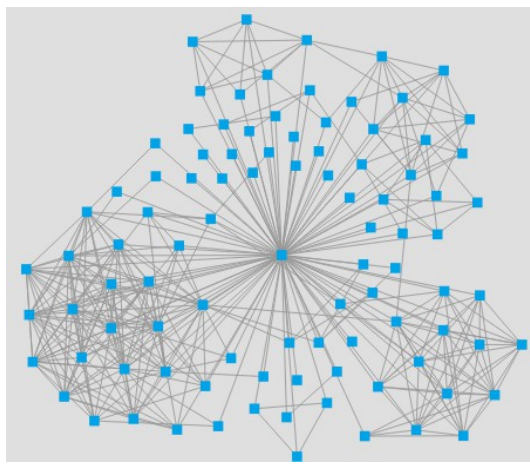
n – количество смежных вершин, у выбранной вершины.

На основе формулы (9) оценивается риск всех сотрудников в социальном графе, и в зависимости от уровня риска ставиться приоритет.

Для иллюстрации работы представлена на рисунке 5 б), где уровень риска указанно соответственно «Высокий» красным, «Средний» оранжевым, «Низкий» зелёным цветами.



а)



б)

Рисунок 5 – Результат работы алгоритма «Оценки организационных рисков компании на основе анализа социального графа сотрудников компании»

Описание метода оценки организационных рисков

Входные данные

– Мнения экспертов о возможном ущербе для бизнеса (ценность сотрудника);

– Экспертные заключения о влиянии одного сотрудника на другого (психологическая особенность, должность, ценность связи);

– База данных сотрудников компании;

– Список сотрудников — должности.

Выходные данные

– Ранжированный список сотрудников.

Ограничения

– Необходимость привлечения экспертов в области информационной безопасности;

– Доступ к внутренним данным организации (База данных сотрудников);

– Необходимость выхода к Интернету;

– Этот метод реализуется программно, а для обеспечения эффективности работы и своевременного обновления требуется привлечение специалиста (программиста);

– Сбор данных из внешних источников может не предоставить большого объёма информации о сотрудниках (связях).

Преимущества и недостатки

Преимущества оценки организационных рисков:

– Оценка организационных рисков используется при диагностике социальной сети организации;

– Сотрудник не рассматривается отдельно от компании, а рассматривается в целом взаимодействие в коллективе и в компании;

– Учитывается особенности взаимоотношений людей в целом (формальные, неформальные);

– Скрытые связи между сотрудниками из внешних источников;

– Учитывается психологические особенности иерархической структуры организации;

– Метод оценки организационных рисков может быть автоматизирован;

– Результаты анализа и оценки организационных рисков позволяют сэкономить время и денежные ресурсы компании для обучения персонала (ранжированный список сотрудников компании по степени компрометации).

К недостаткам относятся следующие пункты:

– Невозможно определить достоверность информации, полученной из внешних источников;

– Оценка может иметь большие погрешности оценки, что может привести к ложным выводам, но лишнее повторное обучение сотрудника нельзя назвать недостатком метода.

Эта методика интересна с точки зрения автоматизации процесса идентификации «уязвимых» сотрудников и дальнейшего процесса их обучения.

Заключение

Компании ежегодно инвестируют миллионы долларов в новейшие продукты безопасности, от межсетевых экранов до систем контроля доступа, но они забывают или не в состоянии инвестировать в свои самые ценные ресурсы для обеспечения своей безопасности — в частности, в своих сотрудников. Слишком часто обучение вопросам информационной безопасности — это событие бывает раз в год и связанно с незанятым и устаревшим материалом, который в значительной степени игнорируется. В результате сотрудники не понимают современных атак и их последствий. Этот пробел в знаниях предоставляет бесконечные возможности для злоумышленников, ставя под угрозу важную информацию организаций. Своевременное выявление пробелов в области информационной безопасности и правильное планирование мероприятий по повышению уровня осведомлённости сотрудников ключ к решению нависшей проблемы. Методика, описанная в данной статье, позволяет идентифицировать «уязвимых» сотрудников и дальнейшего процесса их обучения.

Литература

1. Астахова Л. В., Н. Л. Ульянов. Модель политики управления осведомленностью сотрудников организации в области информационной безопасности. // Наука ЮУрГУ: материалы 67—й научной конференции. Секция технических наук. — С. 678—681.
2. ГОСТ Р ИСО/МЭК 31010—2011. Менеджмент риска. Методы оценки риска [Текст]. — Введ. 2012—12—01. — М.: Стандартинформ: Изд-во стандартов, 2012. — 69 с.
3. Гудкова Д. Н., Демидова Н. Т., Вергелис М. И. Спам и фишинг в третьем квартале 2015 [Электронный ресурс]. — Электронные текстовые данные — Москва, декабрь 2, 2015. — Режим доступа: https://securelist.ru/spam—and—phishing—in—q1—2015/21235/ (Дата обращения 02.01.2018).
4. Гудкова Д. Н., Демидова Н. Т., Вергелис М. И. Спам и фишинг в четвертом квартале 2017. [Электронный ресурс]. — Электронные текстовые данные — Москва, ноябрь 2, 2017. — Режим доступа: https://securelist.ru/spam—and—phishing—in—q4—2017/30565/ (Дата обращения 04.01.2018).
5. Canada/ GetCyberSafe blog. Phishing: How many take the bait? [Электронный ресурс]. — Электронные текстовые данные — Канада, 2017. — Режим доступа: https://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs—2017—10—11—eng.aspx (Дата обращения 10.01.2018).
6. Jonathan C.A. Phishing by the Numbers: Must—Know Phishing Statistics 2017 [Электронный ресурс]. — Электронные текстовые данные — New York, 2017. — Режим доступа: https://blog.barkly.com/phishing—statistics—2017 (Дата обращения 20.11.2017).