• процент затраченных трудовых единиц (от утвержденного в начале проекта).

По указанным метрикам на основе введенных характеристик проекта приложение, основываясь на собственной базе данных, подбирает методологии и инструментарий, соотносящийся с конкретной методологией.

Результат работы приложения поможет начинающим бизнес-аналитику и руководителям проектов в принятии решения относительно разных проектов, сократит временные трудозатраты сотрудников на поиск необходимой информации, тем самым сделав их работу более оптимизированной и эффективной уже в начале карьеры.

Литература

1 Профиль: Бизнес-аналитика и статистика [Электронный ресурс]. – bak.sseu.ru/bakalavriat/profil-biznes-analitika-i-statistika (дата обращения 21.10.2016);

2 Управление проектами и программами в городском хозяйстве и строительстве [Электронный ресурс]. – samara.academica.ru/university/18856-Samarskij-gosudarstvennyj-arhitekturno-stroitelnyj-universitet/vysshee-obrazovanie/826904-upravlenie-proektami-i-programmami-v-gorodskom-hozjajstve-i-stroitelstve (дата обращения 21.10.2016);

3 Программы магистратуры [Электронный ресурс]. – www.sseu.ru/postupayushchim/programmy-magistratury(дата обращения 21.10.2016);

4 Программы вступительных испытаний в магистратуру [Электронный ресурс]. – abiturient.samgtu.ru/programmy-vstupitelnyh-ispytaniy-v-magistraturu (дата обращения 21.10.2016);

Д.Н. Осипова, П.К. Шиверов, М.Н. Осипов

МЕТОДИКА ОЦЕНКИ РИСКОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(Самарский университет)

Введение

Система оценки рисков занимает одну из главенствующих позиций в структуре информационной безопасности. Оценка рисков – это эффективный механизм управления безопасностью, позволяющий оценить, как эффективность существующих средств защиты информации, так и необходимость внедрения новых. Также, оценка рисков помогает при идентификации и оценивании активов компании.

Тем не менее, на данный момент система оценки рисков применяется в большей степени в общем виде, и не существует единых формул и методик для оценки риска применительно к информационной безопасности. Таким образом, целью данной работы и является выведение единой формулы для оценки рис-

ков системы информационной безопасности, а также применение данной формулы на практике для выявления и исправления недостатков.

Актуальность данной работы заключается в том, что наличие выведенной формулы предлагает готовое решение в области оценки рисков для информационной безопасности.

Вывод формулы оценки риска

Для получения результата в виде формулы оценки риска, которая ляжет в основу методики, необходимо предпринять следующие шаги:

1) ввести основные понятия для оценки рисков в информационной системе

2) определить степень значимости угроз информации, для оценки их влияния на результирующую величину, определяющую степень риска.

3) вывести конечную формулу, которая описывает оценку риска для информационных систем.

Важность информации (*I*). Под важностью информации понимается качественная характеристика определяющая ценность информации для пользователя (владельца, собственника информации) [1].

Вся информация, имеющая для компании ценность подразделяется на блоки, каждому из которых дается значение важности. Причем важность блока информации варьируется по абсолютной шкале от 0 до 1. Стоит учитывать, что абсолютного значения важности 1 не достигает ни один блок информации. Максимальное значение представляет собой значение, стремящееся к 1.

Вероятность реализации атаки (P). Является комплексным понятием и складывается из следующих компонентов:

• во-первых, все виды атак.

• во-вторых, система защиты информации (СЗИ).

Каждый элемент СЗИ характеризуется 2 величинами — минимальной вероятностью атаки на данный элемент и максимальной вероятностью.

Вероятность определяется по абсолютной шкале от 0 до 1, аналогично важности информации. Однако допустимым является значение 1 для любого элемента оцениваемой системы, что подразумевает наивысшую вероятность атаки. Исходя из рассмотренных составляющих, выведем формулу оценки риска (*R*), учитывая важность *(I)* каждого элемента системы и вероятность реализации угроз (*P*).

Каждая атака является независимым событием, поэтому для вычисления вероятности реализации угрозы достаточно посчитать вероятность реализации хотя бы одной из возможных атак [2].

Таким образом, вероятность реализации атаки *P* вычисляется:

$$P = 1 - \prod_1^n (1 - P_i), \quad (1)$$

где P_i – вероятность реализации *i*-ой угрозы, *n* – общее количество атак.

Каждая подсистема обладает некоторой степенью важности ($I_{\text{подсист}}$), которая обуславливает заинтересованность злоумышленника в проведении атаки на конкретный элемент системы. Указанную заинтересованность можно обозначить в виде коэффициента:

$$k_{\text{подсист}} = \frac{I_{\text{подсист}}}{\sum_1^m I_j}, \quad (2)$$

где m – общее количество подсистем.

Согласно стоимостной мере риска (*Value at Risk*), оценка производится по формуле

$$R = P \times I \quad (3)$$

Из (2) и (3) следует, что

$$R_{\text{подсист.}} = k_{\text{подсист}} \times P_{\text{общ}} \times I_{\text{подсист}} \quad (4)$$

Тогда

$$R_{\text{общ}} = k_{\text{общ}} \times P_{\text{общ}} \times I_{\text{общ}} = \sum_1^m R_{\text{подсист}j} \quad (5)$$

$$\left(\frac{I_1+\cdots I_m}{I_1+\cdots I_m}\right) \times P_{\text{общ}} \times I_{\text{общ}} = P_{\text{общ}} \times (k_1 I_1 + \cdots + k_m I_m) \quad (6)$$

При сокращении $P_{\text{общ}}$ и $k_{\text{общ}}$, т.к. сумма всех коэффициентов подсистем системы равна 1, получается следующее равенство

$$I_{\text{общ}} = (k_1 I_1 + \cdots + k_m I_m) \quad (7)$$

Отсюда

$$I_{\text{общ}} = k_1 I_1 + \cdots + k_m I_m = \frac{I_1^2+I_2^2+\cdots I_m^2}{\sum_1^m I_j} \quad (8)$$

Следовательно

$$R_{\text{общ}} = (1 - \prod_1^n (1 - P_i)) \times \frac{I_1^2+I_2^2+\cdots I_m^2}{\sum_1^m I_j}$$

Подводя итог, перечислим те преимущества, которые дает проведение анализа рисков в сфере ИБ:

- выявление проблем в сфере безопасности (не только уязвимостей компонент системы, но и недостатков политик безопасности и т.д.)
- анализ рисков позволяет нетехническим специалистам (в частности, руководству организации) оценить выгоды от внедрения средств и механизмов защиты и принять участие в процессе определения требуемого уровня защищенности КС
- проведение оценки рисков добавляет обоснованность рекомендациям по безопасности
- ранжирование рисков по приоритетам позволяет выделить наиболее приоритетные направления для внедрения новых СЗИ, мер и процедур обеспечения ИБ [3]

Выводы и следствия

Оценка рисков – это один из эффективнейших механизмов управления безопасностью в компании. Поэтому вывод формулы оценки риска для ИБ имеет большое значение. Применение формулы, предоставленной в данной работе, позволяет проанализировать систему защиты информации предприятия, выделить уязвимые места СЗИ и произвести расстановку приоритетов в области защищаемой информации для минимизации риска потерь важной информации.

Литература

1. С.А. Нестеров–Анализ и управление рисками в сфере информационной безопасности [Текст]– М.: Санкт-Петербург, 2007. — 47с.
2. ФСТЭК Р. №31 «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» [Текст] – Введ. 2014-03-14
3. ОБЗОР МЕТОДИК АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ / Пугин В. В., Губарева О. Ю. - T-Comm - Телекоммуникации и Транспорт Выпуск № 6 / 2012 – С. 56-57

А.А. Пасюков, Р.И. Баженов

ВНЕДРЕНИЕ СКРЫТЫХ СООБЩЕНИЙ В АУДИО СИГНАЛЫ НА ОСНОВЕ ЭХО-СИГНАЛОВ

(Приамурский государственный университет им. Шолом-Алейхема)

В современном обществе, когда информационные технологии проникают во все сферы жизнедеятельности человека, остро стоит вопрос обеспечения защиты речевой информации и телефонного разговора от угроз неправомерного хищения. В настоящий момент существует достаточно различных средств защиты, которые позволяют защитить такой род информации. И хотя ученые уделяют много времени для совершенствования этой защиты, никому до сих пор не удалось достичь совершенства.

Одним из способов информационной безопасности является защита с помощью стеганографии. Стеганография в отличие от криптографии скрывает сам факт существования информации, которую необходимо защитить от вмешательства посторонних лиц. Скрываемая информация встраивается в некий контейнер, который располагается в безобидном файле любого формата. Это может быть речь, изображение, видео и аудио записи, не привлекающие особого внимания, которые открыто передаются адресату. Нужную информацию может извлечь только получатель.

В ходе работы, планируется разработать способ защиты телефонного разговора по сетевой линии связи IP – телефонию используя спектральные методы.

Многие зарубежные и русские ученые занимались данной проблематикой. В работе Жарких А. А., Пластунов В. Ю. [1] был представлен метод внедрения цифрового водяного знака в аудиосигнал в виде аудиосигнала на основе преобразований конформной алгебры единичного круга. Стародубцев Д. Е., Плашенков В. В. [2] описали алгоритм реализует процедуру интерпретации двоичного потока сообщения как некоторого мелодического контейнера, хранящегося в формате MIDI-файла. Заикин М.А., Гончаров Н.О. [3] описали исследование эффективности метода защиты аудио сигнала при передаче по от-