УДК 541.64

Разработка опросника для выявления потенциального инсайдера в коммерческой организации

Бросалин И.Е., Минакова Н.Н.
Алтайский государственный университет,
iebrosalin@gmail.com, minakova@asu.ru

Аннотация

Предлагается опросник для выявления потенциального инсайдера в коммерческой организации. Сформулированы факторы, характеризующие человека как потенциального инсайдера. Рассмотрены поведенческие признаки, позволяющие отнести сотрудника к потенциальному инсайдеру. Оценены факторы, увеличивающие риск инсайдерства. Предложена система оценки для итогового результата. Анализируются особенности применения опросника.

1. Введение. Обеспечение защиты информации в коммерческой организации – сложная и многогранная задача. Это связано с возрастающим количеством угроз и уязвимостей в информационных системах [1]. Они постоянно видоизменяются, например, угроза безопасности периметра организации трансформируется с физического периметра на виртуальный из-за развития информационных технологий, удовлетворяющих потребности не только бизнеса, но и большого числа пользователей. Изменяются инструменты и меры противодействия, система взглядов на процесс обеспечения информационной безопасности. В современных условиях систему защиты информации в коммерческой организации можно условно разделить на множество взаимодействующих элементов, где чаще всего надёжность определяется прочностью самого слабого элемента [1, 2].

При всем многообразии угроз и уязвимостей неуклонно возрастает доля угроз, связанных с действием человека [3, 4]. В основном это утечка информации, реализуемая по различным каналам [5]. Чаще всего нуждаются в защите персональные данные, коммерческая тайна, стратегия развития или планы на ближайшее время и т.п. Поэтому проблема выявления инсайдера в коммерческой организации чрезвычайно актуальна. Существуют технические средств мониторинга действий пользователей, например, DLP – системы, представляющие из себя комплекс программных продуктов, или различного рода мониторов, отслеживающих трафик и действия [6]. Важнейшей задачей является совершенствование методов периодической оценки сотрудников на возможное инсайдерское поведение. Работы ведется в различных направлениях, например, используется широкий спектр опросников, основанных на предложенной Густавом Юнгом структуре личности [4]. Такие опросники отличаются высокой вариабельностью интерпретаций, так как для точной оценки требуется большой опыт в использовании опросника и довольно глубокие знания в психологии.

В работе предлагается опросник, основанный на минимальном использовании специализированных психологических инструментов, чтобы повысить объективность оценки и снизить зависимость качества результата от интерпретации. Разработка таких опросников требует нетривиальных подходов, так как инсайдерство может быть спровоцировано в процессе деятельности человека в организации.

2. Цель и задачи. Цель работы – разработка опросника, направленного на выявление потенциально опасного сотрудника для организации.

Одна из главных особенностей разработанного опросника заключается в том, что окончательное решение о причислении сотрудника к инсайдерам остаётся за уполномоченным лицом, так как этот вопрос может иметь неоднозначное решение. Роль опросника в этом случае - помогать собирать информации о человеке и предоставлять её в удобном виде для последующего анализа и проверки. Такой подход позволит минимизировать ограничения опросника, например, время прохождения, содержание

вопросов, возможность сотрудника отказаться отвечать на вопрос, выбрав вариант ответа «не знаю». Обстановка и особенности организации процесса опроса также влияют тем или иным образом на результат опроса. Поэтому опросник – это инструмент для сбора и первичной обработки данных для последующего анализа результатов человеком или специализированной экспертной системой.

Задачи работы:

•Сформулировать факторы, характеризующие человека как потенциального инсайдера;

•Выявить поведенческие признаки, позволяющие отнести сотрудника к потенциальному инсайдеру;

• Выделить условия (оценить факторы), увеличивающие риск инсайдерства;

•Разработать опросник, направленный на выявление потенциального инсайдера в организации;

•Предложить систему оценки для итогового результата;

•Разработать программу ЭВМ для сбора данных и первичной обработки информации.

3. Признаки инсайдера. Для повышения результативности выявления инсайдерских черт и оценки риска инсайдерства при непредвиденных обстоятельствах в опросе использованы следующие представления:

-Сотрудник как подверженный эмоциональным всплескам человек, может стать инсайдером в процессе работы в организации из-за непредвиденных обстоятельств, особенностей текущей ситуации и т.п.;

-Сотрудник может быть предрасположен к краже информации в организации из-за психологических особенностей личности (факторы, характеризующие человека как возможного инсайдера);

-Вероятность правдивого ответа сотрудника повышается при уменьшении времени на обдумывание ответа, поэтому предусмотрен учет времени проведения опроса.

4. Факторы, характеризующие сотрудника как инсайдера и условия, увеличивающие риск инсайдерства. Разработанный опросник, содержащий два блока вопросов. Первый блок опросника направлен на выявление мотивационной компоненты, которая может быть сформирована из-за появившихся в процессе работы обстоятельств. В основу первого блока опросника положена классификация InfoWatch [7]. Второй блок оценивает уровень стресса и даёт информацию о характере реакции человека на стресс. В его основе лежит тест Спилберга [8].

Первый блок опросника состоит из трех частей, учитывающих:

•Обстоятельства, которые могут спровоцировать сотрудника на умышленное неправомерное действие или непредумышленное действие, способное нанести ущерб (например, репутационный) коммерческой организации;

•Вопросы, позволяющие оценить возможную мотивацию действий сотрудника, его финансовое положение на текущий момент;

•Вопросы, направленные на выявление неумышленного несоблюдения правил безопасности.

Деление из классификации InfoWatch изменено с учетом поставленных задач. Не используются блоки «Постановка задачи» и «Действия при возможности». Вопрос о том, есть ли у сотрудника цель навредить организации, предлагается анализировать, собирая информацию о возможных факторах, которые могут побудить пойти на нарушение закона и увеличат риск сотрудника стать инсайдером. Эта задача возлагается на блоки «Мотив» и «Корысть». Опросник позволяет уточнить тип инсайдера, соответственно спрогнозировать его возможные действия.

Далее представлены характеристики каждого типа инсайдеров в соответствии с таблицей 1 [8].

Таблица 1 – Виды инсайдеров [8].

Типы инсайдеров	Факторы	
	Мотив	Корысть
Халатный\манипулируемый	-	-
Обиженный\нелояльный	+	-
Подрабатывающий\внедренный	+	+

Халатный. Наиболее распространённый тип внутреннего нарушителя. Обычно сотрудник рядового состава, отличающийся невнимательностью к вопросам безопасности информации. Он часто нарушает правила работы с конфиденциальной информацией – выносит информацию из офиса для работы дома, а потом теряет носитель или допускает доступ члена семьи. Работник действует из лучших побуждений. Однако его попытки сделать «как лучше» ухудшают ситуацию. Ущерб от таких инцидентов трудно предсказать и оценить, так как велик фактор случайности. В случае проблемы такие сотрудники обычно предпочитают обратиться за помощью к старшим коллегам либо к техническим специалистам, которые укажут на их ошибки. Против таких нарушителей действенны простые технические средства предотвращения каналов утечек - контентная фильтрация исходящего трафика в сочетании с менеджерами устройств ввода - вывода.

Манипулируемый. Такие люди часто попадаются на уловки социальной инженерии. Слова (действия) злоумышленника для них являются настолько убедительными, что не так просто увидеть попытку манипуляции. Исходя из своего понимая блага для организации, они ей вредят, нарушая установленные регламенты хранения и движения информации. В случае проблемы обычно действуют как «Халатные инсайдеры». Способы противодействий аналогичны.

Обиженный. Сотрудник может сознательно стремиться нанести вред организации по личным мотивам из-за недостаточного размера материальной компенсации, неподобающего места в корпоративной иерархии, отсутствия элементов моральной мотивации или отказа в выделении корпоративных статусных атрибутов (ноутбук, автомобиль, секретарь и т.п.). Такие сотрудники обычно не собираются покидать организацию, а хотят нанести ей вред. Поэтому столкнувшись с технической невозможностью похищения информации, могут переключиться на уничтожение или фальсификации доступной информации. Стараются сделать всё это тайно. Противодействие таким инсайдерам осуществляется не только средствами защиты от утечек, но работой с кадрами.

Нелояльный. Прежде всего, это сотрудники, принявшие решение сменить место работы или вид деятельности, например, открыть свой собственный бизнес. Они первыми попадают под подозрение, когда заходит речь о внутренних нарушителях. Часто такие сотрудники уносит с собой копии базы клиентов, финансовой базы. Возможно также и кража интеллектуальной собственности. Ключевой особенностью является то, что они пытаются нанести максимальный ущерб компании. Под предлогом производственной необходимости нелояльные сотрудники получают доступ к конфиденциальной информации. Украденные данные могут и не принести вреда организации, так как не всегда удаётся найти тех, кому можно продать информацию. Способы борьбы с такими нарушителями аналогичны способам для категории «Обиженные». Дополнительно рекомендуется присмотр за такими сотрудниками.

Подрабатывающий. Это широкий пласт сотрудников, вступивших на стезю инсайдерства по различным причинам. Сюда включаются люди, решившие подработать на дорогую покупку. Нередки случаи инсайдеров поневоле - шантаж, вымогательство извне не оставляют выбора. Они выполняют приказы третьих сторон. «Подрабатывающие» могут предпринимать самые разнообразные действия при невозможности выполнения поставленной задачи. В зависимости от условий они могут прекратить попытки,

имитировать производственную необходимость. В некоторых случаях могут пойти на взлом, подкуп других сотрудников, чтобы получить доступ к информации любыми другими способами. Однозначные рекомендации дать сложно. Соблюдение политики информационной безопасности позволит минимизировать угрозы.

Внедренный. В отличие от предыдущих типов инсайдеров такой сотрудник старается получить доступ к конкретной информации, которую определяет заказчик. Возможна имитация производственной необходимости, подкуп других сотрудников и т.д. Рекомендации по борьбе с таким видом нарушителей аналогичны рекомендациям категории «Подрабатывающий».

На основании изложенного первый блок разработанного опросника состоит из трёх наборов вопросов:

1. **Мотив.** В этот набор включены вопросы, касающиеся разногласия с начальством, неудовлетворённости работой и т.п. Было важно отделить остальные желания от корыстных мотивов.
2. **Корысть.** Желание иметь более материально обеспеченную жизнь является во многом распространённым. Оно служит мотивацией для правонарушения.
3. **Грамотность.** Это набор вопросов, составленный на тему грамотности в информационной безопасности. Данная оценка выводится отдельно и служит дополнительной характеристикой сотрудника, чтобы облегчить последующий анализ результатов.

Вопросы составлялись с учетом характеристик, указанных в таблице 1 типов инсайдеров. Вопросы формулируются так, чтобы уточнить наличие факторов, повышающих риск инсайдерства. Далее в качестве примера приведены некоторые вопросы по указанным блокам.

Мотив:

1. Вы занимаете руководящую должность?
2. Вам нравится работа?
3. Вас устраивает коллектив?
4. Часто возникают споры с руководством?
5. Вы бы изменили что-нибудь в организации будь у Вас власть?
6. У Вас были выговоры?
7. В компании работает кто-нибудь из Ваших родственников?
8. Вы планируете сменить место работы?

Корысть:

1. Среди Ваших родственников есть желающие работать в этой организации?
2. Вы теряли деньги из-за выговоров от начальства?
3. У Вас есть кредит или ипотека?
4. В Ваших планах есть дорогостоящая поездка?

Грамотность:

1. Часто теряете пропуски, флэшки, документы?
2. Используете свою флэшку, облачные диски на работе?
3. Используете свои почтовый ящик, аккаунт в социальных сетях?
4. Часто задерживаетесь на работе?
5. Бывает такое, что Вы приходите на работу раньше остальных коллег?
6. Вы рассказываете семье, друзьям о своей работе?
7. Бывает такое, что друзья или семья помогают Вам в работе?

Оценка выполняется путем начисления баллов за ответ. Введен ответ «не хочу отвечать». Процедура опроса добровольная, поэтому имеются ограничения на содержание вопросов и возможности получить информацию от работника о себе.

5. Критерии оценки. Предложена система оценки, состоящая из двух частей. В первой части происходит качественное определение наличия признака на основе алгоритма качественной оценки угрозы [9] и оценивается соотношение признаков для рассматриваемой

классификации в таблице 1. Варианты ответов: «да», «нет», «не хочу отвечать» - соответствуют качественным оценкам: «низкий», «средний», «высокий». Пример оценки представлен в таблице 2.

Таблица 2 - Система оценки

Признак/баллы	Да	Нет	Не хочу отвечать	Максимум баллов
Мотив	+2	-2	0	16
Корысть	+2	-2	0	10
Грамотность	+2	-2	0	14

Оценка конечного результата проводилась по критериям, представленным в таблице 3.

Таблица 3 – Качественное определение наличия факторов

Признак/набранные баллы	От 0 до 10	От -1 до -10
Мотив	+	-
Корысть	+	-

Вторая часть состоит из определения вспомогательных критериев, которые необходимы для проверки корректности присвоенного типа инсайдера. Результаты теста Спилберга, время прохождения опроса, количества набранных баллов за набор вопросов «Грамотность» - вспомогательные критерии, позволяющие уполномоченному лицу вынести решение при оценке потенциальной опасности.

6. Предлагаемый опросник. Программа была реализована на языке программирования Java с использованием библиотеки Swing. Процесс опроса состоит из нескольких шагов:

- Заполнение анкеты, где указывается ФИО, должность, сколько лет отработал в организации.
- Опрос. Поле для опроса не имеет отвлекающих надписей. Для повышения внимания к вопросам используются разные фоновые изображения. Пример на рисунке 1.

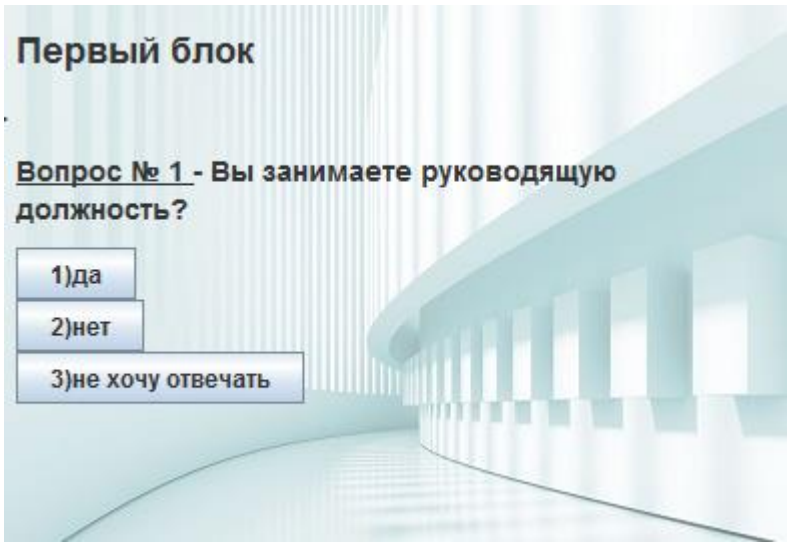

Рисунок 1. Пример вопроса

- Запись результатов опроса в html файл.

Опросник разработан как инструмент для сбора и первичной обработки данных для последующего анализа результатов человеком или специализированной информационной системой. Только по результатам всестороннего анализа делается вывод о причислении сотрудника к потенциальным инсайдерам.

7. Заключение. В работе рассмотрены проблемы, возникающие при выявлении потенциального инсайдера в коммерческой организации. Предложены факторы, которые могут характеризовать человека как потенциального инсайдера. Выявлены поведенческие признаки, позволяющие отнести сотрудника к потенциальному инсайдеру. Выделены условия, увеличивающие риск инсайдерства.

Библиографический список

1. Минакова Н.Н., Поляков В.В., Толстошеев С.Н. Методы технической и правовой защиты информации в сети Интернет. – Барнаул: изд-во Алт. ун-та, 2015. – 155 с.
2. Поляков В.В. Региональные аспекты технической и правовой защиты информации // В.В.Поляков, В.А. Трушин, В.В. Поляков, П.В. Малинин, А.А. Исаев, Т.В. Сидоренко, В.А. Мазуров, А.С. Шатохин, О.С. Терновой, Н.Н. Минакова, И.Н. Загинайлов, П.М. Плетнев. – Изд-во АлтГу, Барнаул, 2013
3. Минакова Н.Н. Анализ биофизических характеристик по результатам обработки полиграмм //Известия Алтайского государственного университета – Барнаул: 2017. – № 1(93). - С. 29 – 34.
4. Лось А. Б., Кабанов А. С. Безопасность бизнеса//Причины, профилактика и методы противодействия инсайдерской деятельности. – 2016. - № 3. - С. 28-35.
5. Андрианов В.В. Обеспечение информационной безопасности бизнеса./В.В. Голованов, С.Л. Зефиров, В.Б. Голованов, Л.А. Голдуев. – Альбина Паблишерс. - М.: 2011. 373 с.
6. Минакова Н.Н., Поляков В.В., Плетнев П.В. Методы и средства защиты информации в коммерческой организации. – Барнаул: изд-во Алт. ун-та, 2016. – 158 с.
7. Гребень Н.Ф.. Психологические тесты для профессионалов– Минск: Соврем.шк., 2007. – 496 с.
8. Экосистема внутренних нарушителей [Электронный ресурс]. URL: http://www.cnews.ru/reviews/free/insiders2006/articles/ecosystem.shtml (дата обращения: 03.10.2017).
9. Методика оценки рисков информационной безопасности [Электронный ресурс]. URL: https://kontur.ru/articles/1691 (дата обращения: 05.10.2017).