ОЛИМПИАДА ШКОЛЬНИКОВ «ШАГ В БУДУЩЕЕ»

НАУЧНО-ОБРАЗОВАТЕЛЬНОЕ СОРЕВНОВАНИЕ «ШАГ В БУДУЩЕЕ, МОСКВА»

Обнаружение инсайдера в организации

ИУ8
«Информационная безопасность»

Выполнила:
Ученица класса 11-2
ГБОУ школы №1501
Захарова Арина
Научный руководитель:
к. т. н., доцент,
зам. зав. кафедры ИУ-8
МГТУ им. Н. Э. Баумана
Троицкий Игорь Иванович

Москва
2021

Содержание

Вступление:

По мере развития и внедрения в повседневную жизнь современных технологий, все больше данных компаний и предприятий переходят в цифровой формат, поэтому важно думать об их безопасности. По данным компании-производителя программного обеспечения для защиты от утечек информации «СёрчИнформ» за первое полугодие 2020 года 100% российских компаний столкнулись с попытками сливов информации. Наиболее частой причиной этого становятся сами сотрудники, причём 60% утечек такого рода - преднамеренные действия сотрудников, сообщает «СёрчИнформ». По данным «Лаборатории Касперского» средний ущерб от утечки для небольших компаний составляет 1,9 млн. рублей, при этом за последний год российские компании в сегменте малого и среднего бизнеса потратили в среднем 4,7 млн. рублей на обеспечение информационной безопасности, что почти в два раза больше чем годом ранее.

На данный момент частные компании и государственные учреждения сталкиваются со всё большими сложностями при защите интеллектуальной собственности. Для выявления и предотвращения потенциальной угрозы - инсайдеров, необходимо организовать слаженную работу команды, состоящую из ИБ специалистов, HR специалистов и юристов. Которые в своей работе используют анализ психологического портрета сотрудника, анализ круга общения, применение технических средств и технологий информационной безопасности.

Проблема: угроза безопасности данных компаний, связанная с инсайдерской деятельностью.

Цель работы: разработать комплекс технических и психологических и мероприятий, направленных на противодействие инсайдерской деятельности.

ПО, необходимое для решения проблемы:

1. PyCharm — интегрированная среда разработки для языка программирования Python.
2. PyQt5 – библиотека Python для создания графического интерфейса.

Задачи:

1. Проанализировать литературные источники, содержащие информацию по следующим вопросам:
   - ✓ Технические методы защиты и предупреждения инсайдерской деятельности
   - ✓ Работа с PyQt5
2. Определить типы инсайдеров
3. Выявить факторы, определяющие предрасположенность человека к инсайдерской деятельности
4. Определить психологические особенности, характерные для инсайдеров
5. Сформулировать критерии для определения потенциального инсайдера по социальным сетям
6. Определить дополнительные технические средства для предупреждения угрозы
7. Написать программу для мониторинга и выявления потенциально опасных действий сотрудника

Ход выполнения работы:

1. Определение типов инсайдеров

Ознакомившись с рядом материалов, дающих классификацию инсайдеров, было принято решение, что в работе будет использоваться классификация, предложенная компанией InfoWatch:

- ✓ Халатный;
- ✓ Манипулируемый;
- ✓ Обиженный;
- ✓ Нелояльный;
- ✓ Подрабатывающий;
- ✓ Внедрённый

Далее предлагаем подробней рассмотреть каждый из представленных типов.

Халатный инсайдер - рядовой сотрудник, который становится причиной утечки информации по собственной неосторожности. Такой человек не имеет злого умысла или мотива, часто наоборот он действует из лучших побуждений, не отдавая отчёт о возможных последствиях своей деятельности. Примером деятельности этого типа можно назвать копирование рабочей информации на личные носители (для работы с ней дома) с дальнейшей утерей.

Манипулируемый инсайдер - рядовой сотрудник, который становится причиной утечки информации из-за чужого воздействия. при помощи социальной инженерии злоумышленник может получить необходимую информацию от манипулируемого инсайдера. Социальная инженерия - это метод (атак) несанкционированного доступа к информации или системам хранения информации без использования технических средств.

Данные типы инсайдеров не имеют злого умысла и часто действуют из лучших побуждений. Причина их инсайдерской деятельности - недостаточная осведомлённость с политикой безопасности компании.

Обиженный инсайдер - работник, считающий, что его профессиональные качества недооценены, и желающий отомстить компании за эту несправедливость. При этом важно отметить, что такой сотрудник не желает покидать компанию, поэтому постарается сделать все тайно, чтобы руководство не узнало. В случае, если это невозможно, данный тип может прекратить попытки. Помимо этого, важно отметить, что обиженный инсайдер определяет ценность информации по своим критериям и сам определяет, кому передать информацию после хищения.

Нелояльный инсайдер - сотрудник, собирающийся сменить место работы или создающий собственный бизнес, также к этой категории можно отнести временных сотрудников. Деятельность таких инсайдеров, чаще всего, не имеет системного характер, они просто стараются унести с собой максимальное количество информации, к которой имеют доступ.

Два данных типа в отличие от предыдущих имеют собственную мотивацию, но, как и первые два, не имеют заказчика. Они сами определяют информацию, которую необходимо похитить, а также пути её сбыта.

Подрабатывающий инсайдер - сотрудник компании, выполняющий определённый заказ за некую плату. В зависимости от ситуации они могут как остановить попытки получения информации, так и пойти на крайние меры, такие как взлом.

Внедренный инсайдер - специально обученные человек, который проникает в компанию с целью кражи определённой информации.

Это самый опасный тип инсайдера, так как он имеет специальную подготовку и практику.

Два последних типа инсайдеров являются наиболее опасными, потому что они имеют конкретный заказ и рынок сбыта информации.

2. Выявление факторов, определяющих предрасположенность человека к инсайдерской деятельности

Можно заметить, что многие типы инсайдеров не будут создавать утечки, если не столкнутся с определёнными факторами. Из этого следует, что необходимо выявить основные факторы, свидетельствующие о склонности человека к инсайдерской деятельности. Стоит отметить, что в данной работе понятие «фактор» обозначает внешние условия или временное состояние человека (например, стресс, болезнь).

Опираясь на вышеупомянутые типы инсайдеров, исследование «Индикаторы поведенческих рисков для выявления инсайдерских краж интеллектуальной собственности» Эрика Шоу и Харли Стока, а также на статью «Показатели личностной предиспозиции к инсайдерской деятельности» М. А. Поляничко можно выделить следующие факторы:

- ✓ Депрессия;
- ✓ Наличие зависимости (алкоголь, наркотики, азартные игры);
- ✓ Финансовые обязательства, долги и кредиты;
- ✓ Изменение адреса (переезд);
- ✓ Смерть близкого человека;
- ✓ Расставание или развод;
- ✓ Понижение в должности;

- ✓ Изменение места работы;
- ✓ Недовольство уровнем заработка.

В своей статье Поляничко также предлагает опросный лист для оценки личностной предиспозиции с использованием метода, разработанным Т. Сааити.

№	Вопрос	Ответы
1	Имеются ли сведения о нахождении сотрудника в депрессивном состоянии?	Нет
		Имеются косвенные сведения
		Имеются сведения о жалобах сотрудника
		Имеется медицинское заключение
2	Наличие данных о наличии алкогольной зависимости	Нет
		Редкие случаи злоупотребления
		Частые случаи злоупотребления
		Был замечен в состоянии алкогольного опьянения на работе
3	Наличие данных о наличии наркотической зависимости	Нет
		Редкие случаи употребления
		Частые случаи употребления
		Был замечен в состоянии наркотического опьянения на работе
4	Наличие данных о наличии зависимости от азартных игр	Нет
		Редкие случаи игр
		Частые случаи игр
		Прогулы работы из-за азартных игр
5	Наличие финансовых обязательств	Нет
		Обязательства ниже дохода
		Обязательства превышают уровень дохода
6	Наличие сведений о переезде	Нет
		Да
7	Наличие сведений о смерти близкого человека	Нет
		Потеря в течение года
		Потеря в течение периода от года до трех лет
8	Наличие сведений о проблемах в личной жизни	Нет
		Имеются сведения о проблемах
		Нахождение в процессе развода/разрыва отношений

Рис. 1 Опросный лист из статьи «Показатели личностной предиспозиции к инсайдерской деятельности»

Данный опросный лист с некоторыми дополнениями может использоваться для выявления уровня предрасположенности к инсайдерской деятельности с опорой на вышеуказанные факторы.

Таблица 1 - Дополнения к опросному листу «Показатели личностной предиспозиции к инсайдерской деятельности»

1	Наличие сведений о недавнем понижении в должности	Нет
		Да
2	Наличие сведений о недавнем или предстоящем изменении места работы	Нет
		Имеются косвенные сведения
		Имеются достоверные сведения
3	Наличие сведений о недовольстве уровнем заработка	Нет
		Имеются косвенные сведения
		Имеются достоверные сведения
4	Частота инцидентов ИБ	Редко
		Иногда
		Часто
5	Наличие сведений о связях с компаниями конкурентами	Нет
		Имеются косвенные сведения
		Имеются достоверные сведения

3. Психологические тестирования

Существенную роль в определении инсайдера может играть психологическое тестирование. В качестве доказательства эффективности методики психологических тестирований можно привести тот факт, что они используются для отбора кандидатов на службу в органы прокуратуры Российской Федерации, о чём написано в «Руководстве по профессиональному психологическому отбору кандидатов на службу в органы прокуратуры Российской Федерации» в пункте 2.3. Как указывает в своей статье «Психологические аспекты информационной безопасности» Валерий Васильевич Бондарев, для выявления инсайдеров нужно

использовать различные инструменты, в том числе опросники, например, тест MBTI (Индикатор типов Майерс-Бриггс). Стоит отметить, что для наиболее точного результата необходимо использовать несколько тестов, описывающих разные качества человека, например**,** комплекс следующих тестов: тест «Соционика» Гуленко и «16-факторный личностный опросник Кеттелла» или Индикатор типов Майерс-Бриггс, тест Гилфорда «Социальный интеллект», «Личностные факторы принятия решений» Корниловой. В данной работе будет рассматриваться последний комплекс тестов.

Начнём с анализа MBTI специалисты SearchInform на ресурсе https://habr.com/ru в публикации «Психология на службе информационной безопасности. Склонность к преступлению» приводят следующую таблицу склонности типов к инсайдерской деятельности.

Таблица 2 - Предрасположенность различных типов личности к инсайдерской деятельности

ISTJ	ISFJ	INFJ	INTJ
ISTP	ISFP	INFP	INTP
ESTP	ESFP	ENFP	ENTP
ESTJ	ESFJ	ENFJ	ENTJ

(E/I – экстраверт/интроверт, S/N – сенсорный/интуитивный, T/F – мыслительный/чувствующий, J/P – решающий/воспринимающий)

Красным отмечены наиболее склонные к инсайду типы, синим имеющие меньшую склонность и белым не склонные к созданию утечек. Стоит заметить, что в своей работе «О результатах тестирования слушателей Академии народного хозяйства по двум

тестам: MBTI и соционика» Меньшикова О.Р. выделяет следующие часто встречающиеся типы:

- ✓ ISTJ, ESTJ, ISTP, INTP, INTJ;
- ✓ *STJ, IST*, I*TJ, IS*J, *STP, E*TJ, I*TP;
- ✓ **TJ, *ST*, *S*J, **TP, I*T*;
- ✓ **T*

Здесь «*» обозначены примерно равновероятные признаки. Назовём тип «полным» если все четыре признака у него однозначно определены. Исходя из этих данных можно сказать, что вероятность встретить неполный тип, больше, чем вероятность встретить полный тип, тогда в предложенную таблицу можно внести корректировку и добавить ещё одну степень склонности к инсайдерской деятельности, которая возникает из-за вероятной неоднозначности трактовки результатов тестирования.

Таблица 3 - Расширенная версия таблицы 2

- Высокая склонность
- Средняя склонность
- Низкая склонность
- Нет склонности

ISTJ	ISFJ	INFJ	INTJ
ISTP	ISFP	INFP	INTP
ESTP	ESFP	ENFP	ENTP
ESTJ	ESFJ	ENFJ	ENTJ

После теста MBTI необходимо пройти тест Гилфорда «Социальный интеллект», он поможет оценить способности человека к социальному взаимодействию. Человек с высоким социальным интеллектом хорошо анализирует ситуацию и поведение людей, он может быть потенциальным манипулятором, что присуще некоторым

типам инсайдеров. Последний тест, который необходимо пройти - «Личностные факторы принятия решений» Корниловой, он призван определить готовность к риску и рациональность тестируемого. К инсайду, как правило, предрасположены люди более импульсивные и склонные к риску при принятии решений. На основании данных тестов можно определить, на сколько человека с данным психотипом склонен к инсайду.

4. Определение круга дополнительных проверок, критерии оценки рисков

Ещё одним этапом по определению инсайдера является проверка резюме. Особое внимание стоит уделить кандидатам, которые работали в компаниях конкурентах или часто меняли место работы. Также необходимо проверять социальные сети сотрудника, ключевыми параметрами проверки являются бывшие места работы, места работы друзей, подписки и публикации, свидетельствующие о материальных трудностях, алкогольной или наркотической зависимости, увлечении азартными играми и экстремальными видами спорта.

Дополнительным средством обеспечения защиты от инсайдерских угроз является проверка сотрудника при помощи полиграфа, стоит отметить, что данную процедуру целесообразно проводить только с сотрудниками, которые получают доступ к наиболее важной информации.

5. Рекомендации по проверке сотрудников

Опираясь на описанные выше проверки, можно составить комплекс мероприятий, направленных на определение инсайдера. При

трудоустройстве или изменение в должности можно говорить о следующем ряде мер:

- ✓ HR отдел даёт соискателю пройти психологические тесты MBTI, «Личностные факторы принятия решений» и «Социальный интеллект», результаты передаёт отделу ИБ;
- ✓ ИБ специалист проводит анализ:
  - Социальных сетей;
  - Предыдущих мест работы;
  - Родственных связей;
  - Факторов, определяющих предрасположенность к инсайдерской деятельности;
  - Инцидентов ИБ;

  Результаты анализа заносятся в опросник «Показатели личностной предиспозиции к инсайдерской деятельности»;
- ✓ При необходимости сотрудник проходит проверку на полиграфе;
- ✓ Полученные данные проходят обработку (описание алгоритма приведено в пункте 6), результатом которой является оценка предрасположенности к инсайдерской деятельности.

После прохождения этих процедур вероятность того, что кто-то из сотрудников является инсайдером будет значительно снижена, но важно продолжать работу и применять следующие меры защиты.

Специалистам по информационной безопасности совместно с юридическим отделом необходимо разработать политику конфиденциальности компании. Также, юридическому отделу стоит проводить регулярные беседы с сотрудниками на тему конфиденциальности данных, в которых юристы будут объяснять, что можно делать с информацией компании. Помимо этого, нужно вести длительный мониторинг сотрудников, для определения наличия факторов, влияющих на склонность к инсайдерской

деятельности. Кроме того, необходимо использовать превентивные меры защиты, в частности DLP-систему (Data Leak Prevention).

6. Методика расчёта склонности к инсайдерской деятельности

Полученные в ходе проверок результаты обрабатываем для определения уровня склонности сотрудника к инсайдерской деятельности. В данном разделе представлен алгоритм обработки всех проверок.

При выполнении данного алгоритма все полученные результаты проверок преобразуем в коэффициенты согласно приведённым ниже методам:

- ✓ Значения коэффициента психотипов (k_1) принимаем в диапазоне от 0 до 1, где 0 - минимальная склонности, 1 - максимальная. Распределение коэффициентов приведены в таблице № 4

Таблица № 4 - Коэффициенты психотипов

Результат тестирования	Значение коэффициента k_1
ISTJ, ISFJ, INTJ, ISFP, INFP, ENFP, ENTP (Нет склонности)	0
ESTJ, INTP (Низкая склонность)	0.33
ISTP, INFJ, ESFJ, ENFJ, ENTJ (Средняя склонность)	0.67
ESTP, ESFP (Высокая склонность)	1

- ✓ Коэффициент социального интеллекта (k_2) и коэффициент склонности к риску (k_3) рассчитываем следующим образом:

полученный численный результат тестирования делим на максимальный возможный.

- ✓ Следующим этапом рассчитываем коэффициент предрасположенности к инсайдерской деятельности на основании выявленных факторов (k_4).

Расчёт данного коэффициента производим следующим образом:

1. Для каждого вопроса вводим весовой коэффициент, чтобы определить значимость заданного критерия.

В основу метода расчёта весовых коэффициентов лёг метод анализа иерархий (МАИ) Томаса Саати. МАИ широко используется управленцами при принятии решений, он позволяет из нескольких альтернатив выбрать вариант, наиболее согласующийся с представлением лица, принимающего решение. Реализацию данного метода можно разделить на несколько этапов, опишем их для нашего случая:

- ➢ Определение цели.

Цель: установить предрасположенность к инсайдерской деятельности на основании выявленных ранее факторов.

- ➢ Выделение основных критериев и альтернатив.

Критерии: вопросы опросного листа «Показатели личностной предиспозиции к инсайдерской деятельности»

Альтернатив нет, конечный результат всегда один - численное значение предрасположенности.

- ➢ Построение иерархии: дерево от цели через критерии к альтернативам.

Рис 3. Иерархия

- Построение матрицы попарных сравнений критериев по цели и альтернатив по критериям, Применение методики анализа полученных матриц.

Шаг 1: Заполним матрицу сравнений числами, обозначающими превосходство i-ого критерия (строка) над j-ым (столбец).

Таблица 4 - Значения для заполнения матрицы

Значение ячейки	Пояснение
1	Одинаковая значимость i и j
3	Немного большая значимость i по сравнению с j
5	Более высокая значимость i по сравнению с j
7	Очень высокая значимость i по сравнению с j
9	Максимальная значимость i по сравнению с j

Значения 1/3, 1/5, 1/7, 1/9 эквиваленты значениям 3, 5, 7, 9 при большей значимости j по сравнению с i.

Шаг 2: Для каждой строки рассчитаем локальный вектор приоритетов, он же весовой коэффициент. Каждый строке матрицы ставим в соответствие её среднее геометрическое, суммируя

полученные значения, делим среднее геометрическое каждого элемента на эту сумму, конечное число и есть весовой коэффициент (вектор локального приоритета).

Шаг 3: Проверяем согласованность полученной матрицы. Для этого рассчитываем индекс согласованности (ИС) по следующей формуле:

$$\text{ИС} = \frac{\lambda_{max} - n}{n-1} \quad (1)$$

где n - размерность матрицы, а λ_{max} вычисляется по следующему алгоритму: Сумма элементов первого столбца умножается на первый весовой коэффициент, второго на второй и т. д. (эти значения записаны в столбец «λ»), полученные значения суммируются.

Определяем случайную согласованность (СС) матрицы, это табличная величина.

Таблица 5 - Случайная согласованность

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0,00	0,00	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48	1,56	1,57	1,59

В нашем случае СС = 1,56.

После этого найдём отношение согласованности (ОС).

$$\text{ОС} = \frac{\text{ИС}}{\text{СС}} \quad (2)$$

Если ОС > 0,1, матрица рассогласована. Приведённая нами матрица согласована.

Таблица 6 - Матрица согласованности факторов склонности к инсайдерской деятельности и вычисления

Критерий	Депрессивные состояния	Алкоголизм	Наркомания	Игромания	Долги	Переезд	Смерть близкого	Семейные проблемы	Понижение	Изменение места работы	Недовольство уровнем заработной платы	Частота инцидентов ИБ	Связь с конкурентами		Среднее геометрическое	Весовые коэффициенты	λ	
Депрессивные состояния	1	1/5	1/5	1/5	1/5	3	1/3	1	1/9	1/7	1/7	1/7	1/7		0,283	0,014	0,927804847	λmax
Алкоголизм	5	1	1	1	1	5	3	5	1/5	1/3	1/9	1/9	1/9		0,771	0,039	1,098926163	14,70497466
Наркомания	5	1	1	1	1	5	3	5	1/5	1/3	1/5	1/5	1/5		0,884	0,045	1,258570514	ИС
Игромания	5	1	1	1	1	5	3	5	1/5	1/3	1/5	1/5	1/5		0,884	0,045	1,258570514	0,142082222
Долги	5	1	1	1	1	5	3	5	1/5	1/3	1/5	1/5	1/5		0,884	0,045	1,258570514	СО
Переезд	1/3	1/5	1/5	1/5	1/5	1	1/3	1	1/9	1/7	1/5	1/5	1/5	Вычисления	0,258	0,013	0,934539185	1,56
Смерть близкого	3	1/3	1/3	1/3	1/3	3	1	1	1/7	1/3	1/9	1/9	1/9		0,402	0,021	0,937127686	ОС
Семейные проблемы	1	1/5	1/5	1/5	1/5	1	1	1	1/9	1/3	1/7	1/9	1/9		0,290	0,015	0,932986977	0,091077706
Понижение	9	5	5	5	5	9	7	9	1	1/3	1	1/3	1/3		2,456	0,125	1,537324225	
Изменение места работы	7	3	3	3	3	7	3	3	3	1	1/3	1	1		2,240	0,148	1,278098728	
Недовольство уровнем заработной платы	9	5	5	5	5	9	7	9	1	3	1	1/3	1/3		2,908	0,148	1,429681708	Матрица согласована
Частота инцидентов ИБ	7	5	5	5	5	9	7	9	3	1	3	1	1		3,675	0,187	0,926386799	
Связь с конкурентами	7	5	5	5	5	9	7	9	3	1	3	1	1		3,675	0,187	0,926386799	
Сумма	64,333	27,933	27,933	27,933	27,933	71,000	45,667	63,000	12,276	8,619	9,641	4,943	4,943		19,810	1,034		

- Определение весов альтернатив по системе иерархии (при наличии альтернатив). В нашем случае не выполняется.

Таким образом, мы получили весовые коэффициенты. Для каждой конкретной компании, исходя из её предпочтений, может составляться своя матрица попарных сравнений.

2. Для каждого ответа на вопрос в опроснике назначаем стоимость от 0 до 100, где минимальный балл даётся за отрицательный ответ, максимальный балл за положительный.
3. Баллы за каждый вопрос умножаются на соответствующий весовой коэффициент, затем полученные значения суммируются. Эта сумма делится на максимальную возможную, полученное число и есть коэффициент предрасположенности (k_4).

После определения коэффициента психотипа (k_1), коэффициента социального интеллекта (k_2), коэффициента склонности к риску (k_3) и коэффициента предрасположенности (k_4), рассчитаем уровень склонности к инсайдерской деятельности.

1. Для каждого полученного коэффициента вводим весовой коэффициент, чтобы определить значимость заданного критерия.

Мы уже подробно рассматривали способ получения весовых коэффициентов, поэтому ниже приведём только матрицу сравнений и вычисления.

Таблица 7 - Матрица согласованности типов проверок и вычисления

Критерий	Психотип	Социальный интеллект	Склонность к риску	Предрасположенность	Вычисления	Среднее геометрическое	Весовой коэффициент	λ	ИС
Психотип	1	3	5	1		1,967989671	0,37754424	0,956445407	0,032012763
Социальный интеллект	1/3	1	3	1/5		0,668740305	0,128292873	1,197400152	ОС
Склонность к риску	1/5	1/3	1	1/5		0,339808849	0,06518981	0,912657345	0,9
Предрасположенность	1	5	5	1		2,236067977	0,428973077	1,029535384	СС
Сумма	2,53333333	9,333333333	14	2,4		5,212606803	1		0,035569736

2. Каждый из коэффициентов k_1, k_2, k_3, k_4 умножаем на соответствующий весовой коэффициент (p_1, p_2, p_3, p_4) и на 100, после чего складываем эти значения и получаем конечный результат - уровень склонности к инсайдерской деятельности от 0

до 100, где минимальное значение означает наименьшую склонность, а максимальное - наибольшую.

Для упрощения расчётов напишем программу обработки данных проверок на языке Python.

7. Алгоритм определения инсайдера на основании комплекса проверок

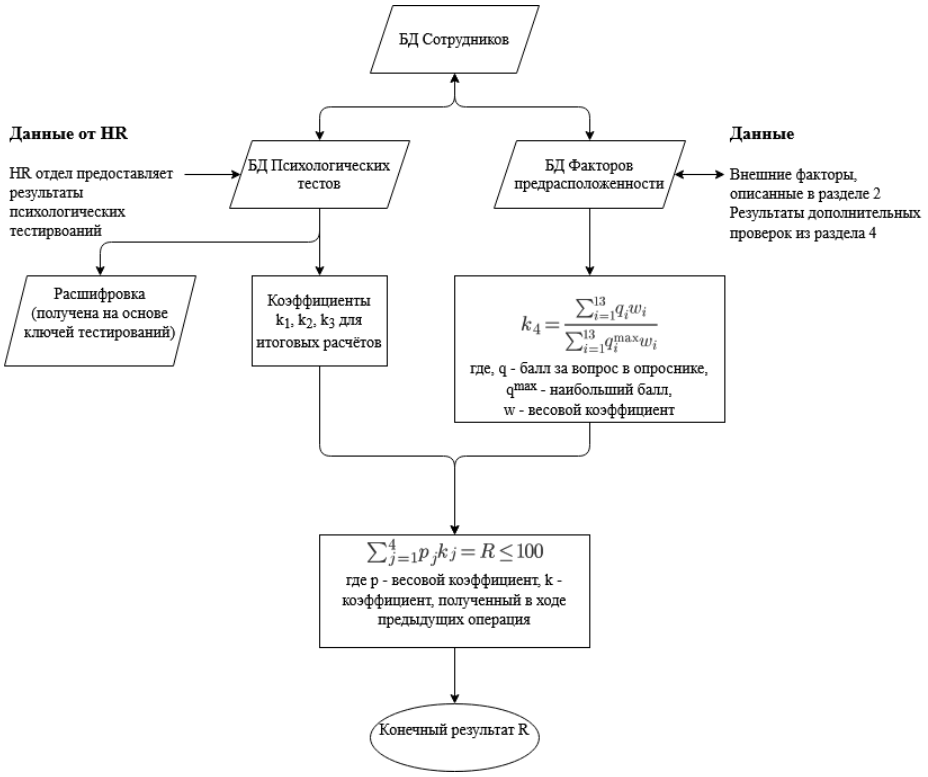

Рис. 3 Блок схема алгоритма

Из приведённого выше алгоритма видно, что данные результатов психологических тестирований сотрудников загружаются в базу данных, после чего по ключам и таблице 3 даётся расшифровка результатов тестирований, коэффициентам k1, k2, k3 присваиваются значения от 0 до 1 на основании расшифровки.

Во вторую базу данных - БД Факторов предрасположенности к инсайдерской деятельности, с помощью опросного листа заносятся результаты проверки социальных сетей, родственных связей, резюме,

инцидентов ИБ и остальные данные проверок, после чего данный опросник расшифровывается по следующему принципу: суммируются баллы за ответ на вопросы q помноженные на соответствующие весовые коэффициенты w (весовые коэффициенты подбираются исходя из предпочтений и приоритетов компании заказчика), после чего полученная сумма делится на максимальный результат, таким образом получается коэффициент k4.

Для определения склонности сотрудника к инсайдерской деятельности используется следующая схема вычислений: k_1, k_2, k_3, k_4, умножаются на соответствующие весовые коэффициенты p_1, p_2, p_3, p_4, $\sum_{j=1}^{4} p_j \le 100$ (3) (данные весовые коэффициент также подбираются исходя из предпочтений компании), полученные произведения суммируются и получается число R ($0 \le R \le 100$), R = 100 - наибольшая склонность к инсайдерской деятельности, R = 0 - наименьшая склонность.

8. Интерфейс и программный код

В данном разделе представлено описание функционала.

Приветственное окно:

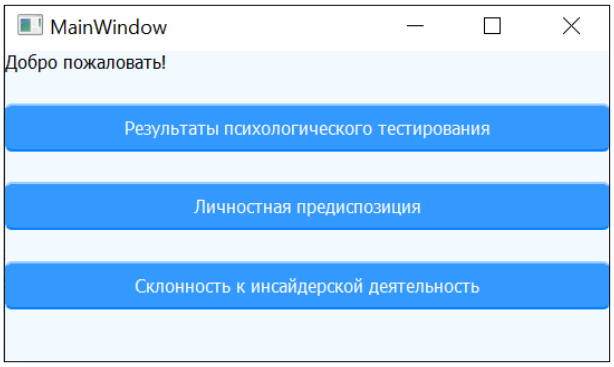

Рис. 4 Приветственное окно

Функционал: Переход к основным окнам программы.

Окно «Результаты психологического тестирования»

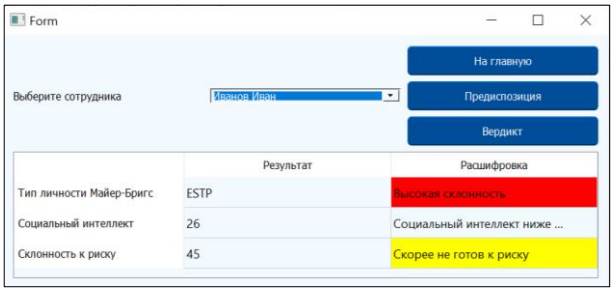

Рис. 5 «Результаты психологического тестирования»

Функционал: Вывод результатов психологического тестирования с комментариями.

Окно «Личностная предисозиция»

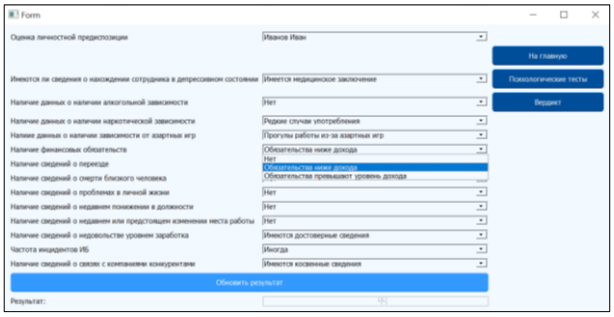

Рис. 5 Окно «Личностная предисозиция»

Функционал: Заполнение и редактирование опросного листа «Показатели личностной предиспозиции к инсайдерской деятельности» и вывод уровня предиспозиции.

Окно «Вердикт»

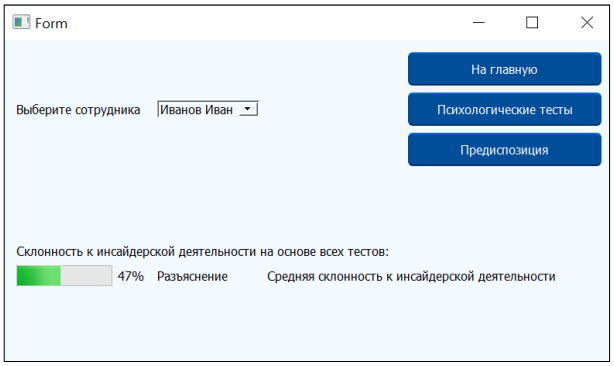

Рис. 6 Окно «Вердикт»

Функционал: Вывод итоговой склонности к инсайдерской деятельности.

9. Машинное обучение

Сложности в подготовительной работе для написания программы, производящей расчёт, наталкивают на мысль о поисках альтернативных способах обработки результатов. Наиболее подходящим вариантом решения этой проблемы является машинное обучение. Для обработки результатов тестирования можно использовать различные алгоритмы, в данной работе будет использоваться дерево решений. Этот алгоритм поддерживает разные форматы параметров, то есть данные не нужно будет предварительно обрабатывать. Также результаты обучения этой модели формирует довольно понятные правила классификации, которые далее можно анализировать.

В открытом доступе нет данных, подходящих для обучения дерева, поэтому для тренировки модели были взяты данные 25 опрошенных и данные ещё 5 человек для проверки обученной модели. Этих данных достаточно для демонстрации принципа работы дерева решений.

Таблица 8 – Данные для обучения

№	MBTI	Социальный интеллект	Склонность к риску	Результат	Обучающее значение
1	ENFP	3	63	12	0
2	ESTJ	3	66	24	0
3	INFJ	4	39	38	1
4	ESTJ	4	26	24	0
5	ENTP	3	56	11	0
6	ENFP	3	67	12	0
7	INTJ	2	70	9	0
8	ISFP	4	34	12	0
9	ENFP	3	85	13	0

10	ESTJ	3	53	23	0
11	ISTJ	3	39	10	0
12	ISTJ	3	29	9	0
13	ENTJ	4	54	39	1
14	ESTP	2	78	48	1
15	ESTJ	3	37	22	0
16	ESFJ	3	51	36	1
17	INFP	4	60	14	0
18	ESTJ	4	49	25	1
19	INTJ	4	44	13	0
20	ESTJ	4	40	13	0
21	ISTJ	4	54	13	0
22	ESFJ	3	45	13	0
23	ESTJ	2	54	36	1
24	ISTP	4	53	21	0
25	ENTP	3	100	14	0
26	ENFP	3	44	10	0
27	INFJ	4	54	39	1
28	ISFP	3	64	12	0
29	ESTJ	5	48	27	1
30	INFJ	4	52	38	1

В результате обучение получилось следующее дерево.

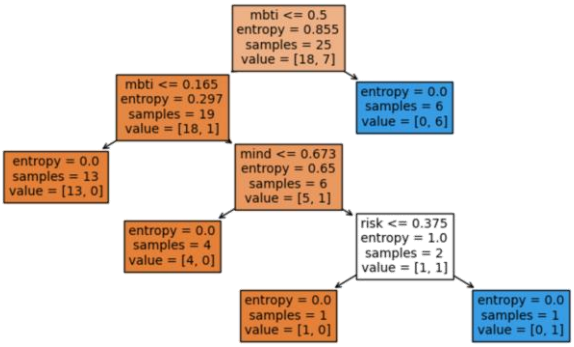

Рис. 7 Дерево решений

Сравним предложенные в данной работе методы обработки результатов тестирований: аналитический подход и машинное обучение. Для наглядности достоинства и недостатки каждого выделены зеленым и красным цветом соответственно.

Таблица 9 – Сравнение аналитического подхода и машинного обучения при выполнении задачи обнаружения инсайдера

Критерий\Метод	Аналитический подход	Машинное обучение
База размеченных данных	Не нужна	Нужна
Трудоемкость подготовительной работы	Высокая	Низкая
Обрабатываемые закономерности	Предустановленные специалистом	Выявленные алгоритмом
Выдаваемый ответ	Процентная вероятность и однозначный ответ	Однозначный ответ

На данный момент нельзя сказать, какой метод лучше, поэтому оба подхода могут использоваться в работе специалиста по информационно безопасности.

Выводы:

1. Разработан комплекс мероприятий, направленных на обнаружение инсайдера в организации.
2. Создан алгоритм для численного расчёта склонности к инсайдерству на основе проверок из разработанного комплекса, адаптируемый под требования каждой конкретной организации.
3. Реализован программный продукт, позволяющий на основе представленного комплекса мероприятий рассчитать склонность к инсайдерской деятельности.
4. Произведено качественное сравнение двух подходов обработки данных тестирований: аналитического и машинного.

Источники:

1. https://www.infowatch.ru/products/prediction
2. https://www.devicelock.com/ru/products/technology.html
3. https://habr.com/ru/post/440838/
4. https://searchinform.ru/blog/2020/08/18/itogi-polugodiya-v-94-sluchaev-iz-organizacij-utekli-poleznye-dlya-moshennikov-dannye/?fbclid=IwAR1tAlLgOePEAY1_FunX219mSKoZdP6xMIur3ElVCAcr4xAr3dCYOuk1YPo
5. https://searchinform.ru/uploads/sites/1/2020/08/incidenty-vnutrennej-bezopasnosti-v-rossijskih-kompaniyah-pervoe-polugodie-2020.pdf
6. https://hr-portal.ru/article/kak-obnaruzhit-potencialnogo-insaydera
7. Т. И. Маркова, К. В. Захарова Ксения «Классификация инсайдеров»
8. Е.А. Мамочка «Типы личности преступника-инсайдера»
9. М. А. Поляничко «Показатели личностной предиспозиции к инсайдерской деятельности»
10. https://www.crn.ru/news/detail.php?ID=61449
11. https://edu.tltsu.ru/sites/sites_content/site216/html/media67140/lec1_is-2_2020%20(1).pdf