УДК 004.056 DOI: 10.17587/it.26.222-230

А. С. Кабанов, канд. техн. наук, доц., e-mail: kabanov_as@mail.ru,
Московский институт электроники и математики имени А. Н. Тихонова
Национального исследовательского университета "Высшая школа экономики"

Оптимизация организационной структуры предприятия с учетом противодействия инсайдерской деятельности

Рассматриваются различные подходы к оптимизации организационной структуры предприятия и обоснована актуальность данной задачи с точки зрения защиты от инсайдерской деятельности. Предложен алгоритм определения места подразделения противодействия инсайдерской деятельности в организационной структуре предприятия. Показан прагматичный подход к оценке необходимости и стоимости внедрения средств противодействия инсайдерской деятельности. Приведено условие экономической целесообразности внедрения средств противодействия инсайдерской деятельности, а также предложены подходы к оценке инсайдерской информации и сформулированы основные выводы. Статья носит аналитический характер и может быть полезна руководителям служб информационной безопасности, преподавателям, аспирантам и студентам вузов.

Ключевые слова: *организационная структура предприятия, инсайдер, инсайдерская деятельность, ценность инсайдерской информации*

Введение

Все предприятия обладают организационной структурой, разработанной на этапе их создания и откорректированной в процессе функционирования. Всякая организационная структура может быть представлена в виде схемы, отдельными блоками которой будут выступать директор или руководитель предприятия, структурные подразделения предприятия, отдельные управленческие единицы и связи между ними.

Американский ученый Питер Друкер показал, что не может быть одной "единственно правильной" организационной структуры. Для каждого предприятия существует своя, оптимальная именно для него организационная структура. Оптимальна только та организационная структура, которая обеспечивает наиболее эффективную реализацию стратегии предприятия по достижению поставленной перед ним цели [1].

Следует отметить, что с точки зрения экономистов организационная структура должна быть оптимальна для достижения экономических целей предприятия. Данный подход не дает информации о том, как должна быть построена организационная структура, поскольку экономическая цель не отражает процессы, протекающие на предприятии. Но именно продукция и процессы, связанные с ее созданием, производством и реализацией, приносящие предприятию экономический эффект, обеспечивают достижение поставленной экономической цели и определяют организационную структуру. А сама продукция и все связанные с ней процессы, в свою очередь, определяются стратегией предприятия. Таким образом, "стратегия определяет структуру" [2]. Очевидно, что в свете современных угроз информационной безопасности становится актуальной задача противодействия инсайдерской деятельности, причем данная задача непосредственно влияет на процессы, протекающие на предприятии по достижению, в том числе, экономических целей.

Вопросы организационной структуры начинаются с разработки стратегии предприятия. Если стратегия изменяется, возможно, потребуется оптимизация организационной структуры под новую стратегию. Очевидно, что с точки зрения защиты от инсайдерской деятельности целесообразно оценить ценность данной информации (ее влияние на стратегию предприятия). После оценки ценности информации и принятия решения по противодействию возникает задача поиска оптимальной организационной структуры предприятия с учетом обеспечения защиты от инсайдерской деятельности.

В классическом понимании целесообразность проведения оптимизации определяется на основе отраслевых показателей, внутренней информации или внешней оценки. Очевидно, что целесообразность проведения оптимизации организационной структуры предприятия с точки зрения защиты от инсайдерской деятельности имеет смысл, только если эта оптимизация не приводит к нарушению стратегических целей (например, ухудшению экономических показателей).

Актуальным вопросом, рассмотренным в данной статье, является определение места подразделения противодействия инсайдерской деятельности (ПИД) в организационной структуре предприятия. В настоящее время

имеется несколько распространенных схем размещения подразделения ПИД в организационной структуре, но, по мнению автора, для некоторых типов предприятий пул вариантов можно значительно сократить (полагаясь на здравый смысл), при этом, безусловно, каждое предприятие индивидуально и может иметь свою специфику.

Следует отметить, что, несмотря на большое число иностранных и отечественных публикаций по проблемам ПИД, все они преимущественно сводятся к анализу средств противодействия (SIEM и т.д.) и разработкам подходов к классификации инсайдеров в целях более эффективного противодействия (например, работы [3, 4]). Вопросы изменения организационной структуры предприятия для противодействия инсайду практически не затрагиваются в отечественной и зарубежной литературе, а лишь изредка упоминаются. В некоторых работах рассматривают различные по размеру предприятия с точки зрения внедрения тех или иных средств противодействия (например, [5]). И это несмотря на то, что нередко оптимизация структуры предприятия может привести к отсутствию необходимости внедрения средств защиты от инсайдерской деятельности. Определение ценности инсайдерской информации редко встречается в публикациях и носит преимущественно очень формальный характер.

Учитывая актуальность данной проблемы, настоящая статья посвящена следующим основным вопросам.

1. Оптимизация организационной структуры предприятия с точки зрения защиты от инсайдерской деятельности.

2. Определение места подразделения ПИД в организационной структуре предприятия.

3. Оценка ценности инсайдерской информации.

1. Построение системы противодействия инсайдерской деятельности с учетом стратегических целей предприятия

После определения стратегических целей и формирования организационной структуры предприятия первостепенной задачей (с точки зрения оптимизации по противодействию инсайду) лиц, ответственных за ПИД, является создание реестра соответствующей информации с оценкой ее стоимости (места в организационной структуре), а также выбор средств ПИД и определение стоимости их внедрения. Следует отметить, что тип информации (ограниченного и неограниченного распространения) достаточно часто не влияет на ценность информации. Нередко открытая информация представляет собой значительно больший "интерес" и ценность для инсайдера, чем информация ограниченного распространения. Например, открытая информация о компаниях партнерах и условиях сделок для организации-конкурента намного "интереснее", чем защищаемые законом и обрабатываемые специальным образом с использованием средств защиты персональные данные.

После создания соответствующего реестра для предприятия возможны три стратегии, выбор которых зависит от внутренней структуры организации (возможности оптимизации), а также специфики реализации технологических и бизнес-процессов, а именно:

1. Для небольших организаций либо организаций, в которых инсайдерская информация достаточно компактно сосредоточена (в силу внутренней структуры и реализации технологических/бизнес-процессов), защита от инсайдерской деятельности может быть сведена к оптимизации структуры в части обработки данной информации. Например, если инсайдерской информации немного, и ее концентрация в одном месте не приводит к нарушению технологических и бизнес-процессов организации, то целесообразно поместить ее в одно помещение одного подразделения с доступом узкого круга доверенных лиц, а также в случае необходимости реализовать достаточно недорогие организационно-технические меры защиты. Кроме того, необходима разработка и утверждение порядка доступа к инсайдерской информации, правил соблюдения ее конфиденциальности, а также создание (определение, назначение) структурного подразделения (должностного лица), в обязанности которого входит осуществление контроля. Данная стратегия, как правило, не требует значительных финансовых затрат (в основном затраты организационные), и реализация систем ПИД достаточно широко описана в различных трудах, например [6—9].

2. Для инфраструктурно сложных предприятий необходимо провести оценку на предмет возможности оптимизации с точки зрения защиты от инсайдерской деятельности, например, свести все звенья, обрабатывающие инсайдерскую информацию, в одном защищенном месте. Очевидно, что если стоимость изменения организационной структуры превышает стоимость ущерба от инсайдерской деятельности, то реорганизация не имеет смысла. Следовательно, если инфраструктурно сложное предприятие нельзя свести к первому типу, то данное предприятие принадлежит к следующему типу.

3. Для больших, инфраструктурно сложных, разветвленных организаций, в которых инсайдерская информация сильно рассредоточена (в силу специфики реализации технологических/бизнес-процессов), целесообразность внедрения различных средств ПИД необходимо предварительно сопоставить со стоимостью утечки инсайдерской информации и стоимостью средств ПИД. Внедрение средств ПИД имеет экономический смысл при выполнении принципа разумной достаточности [10], а именно следующего условия:

$$C_{\text{СПИ}} < C_{\text{риск}},$$

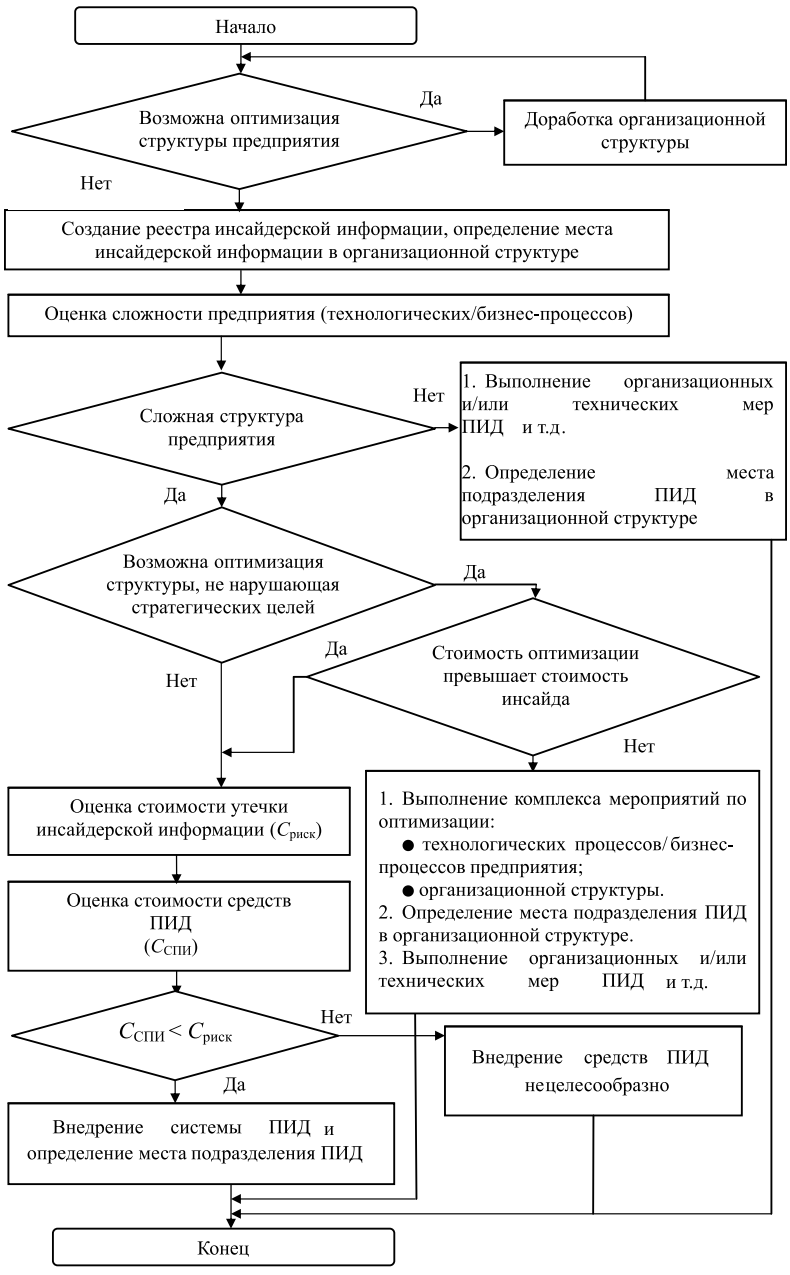

Рис. 1. Алгоритм внедрения средств противодействия инсайду

где $C_{\text{СПИ}}$ — стоимость внедрения средств ПИД; $C_{\text{риск}}$ — стоимость утечки инсайдерской информации для организации.

Следует отметить, что в процессе расчета $C_{\text{риск}}$ в его стоимость (помимо стоимости закупки и внедрения средств ПИД) нередко необходимо включить так называемые репутационные риски организации.

При условии $C_{\text{СПИ}} \geqslant C_{\text{риск}}$ внедрение средств ПИД бессмысленно с точки зрения экономического эффекта. В этом случае, как вариант, возможно построение графа передачи инсайдерской информации между средствами обработки в целях проведения его оптимизации для уменьшения стоимости $C_{\text{СПИ}}$ либо приведения к организации первого типа.

Алгоритм выбора средств противодействия отображен на рис. 1.

Далее рассмотрим подход к определению сложности организации. Для сложных организаций характерна разветвленная структура с большим числом элементов (средств обработки информации, филиалов и т.д.). Точечные решения для таких организаций не всегда применимы и эффективны. При этом сетевые программно-аппаратные средства защиты (в первую очередь SIEM-системы, а также DLP и т.д.) являются более дорогими в части закупки и внедрения. Поскольку интерес представляет только инсайдерская информация, которая хранится, обрабатывается и передается в/между средствами обработки, следовательно, оценка сложности организации тождественна инфраструктурной сложности совокупности данных систем и связей между ними. Таким образом, сложность организации (инфраструктуры) можно оценить, используя теорию графов, где вершины соответствуют отдельным средствам обработки инсайдерской информации, а ребра определяют информационное взаимодействие между ними [11]. Веса ребер графа определяют объем и частоту передаваемой инсайдерской информации. Наличие разных типов взаимодействия определяет множество инфраструктурных графов $G_k = \langle V_k, E_k, W_k \rangle$, где V_k — множество вершин графа; E_k — множество ребер графа; W_k — вес ребер графа; k — тип взаимодействия.

Объединенный граф инфраструктуры имеет вид

$$G = \bigcup_{k=1}^{K} G_k = \langle V, E, W \rangle,$$

где $V = \bigcup_{k=1}^{K} V_k$; $E = \bigcup_{k=1}^{K} E_k$; K — число типов взаимодействия.

Вес объединенного графа для каждого $v_{ij} \in V$ ребра определяется суммой весов исходных графов $w_{ij} = \sum_{k=1}^{K} w_{ij}^k$.

Таким образом, получив граф средств обработки инсайдерской информации и связей между ними, необходимо провести оценку сложности предприятия. Создание указанного графа для некоторых небольших организаций первого типа позволит решить оптимизационные задачи, например, для сосредоточения инсайдерской информации в одном месте и т.д. Под структурной сложностью инфраструктуры предприятия будем понимать свойство, оценивающее размерность такого объединенного графа, многообразие маршрутов между его вершинами, число циклов, близость между вершинами и др.

Необходимо сформулировать требования, которым должен удовлетворять объединенный граф инфраструктуры, чтобы организацию можно было отнести к одному из типов.

На этапе создания реестра инсайдерской информации необходима идентификация всех вершин графа, являющихся средствами обработки инсайдерской информации ($N_{\text{СОИИ}}$). Также должна быть определена максимальная вместимость кластеров средств обработки инсайдерской информации, требующих выполнения недорогостоящих организационно-технических мер защиты информации ($N_{\text{мест}}$), а также число кластеров в конкретной организации (L).

Таким образом, для определения инфраструктурной сложности организации необходимо проверить три условия:

1. $N_{\text{СОИИ}} \leqslant \sum_{i=1}^{L} N_{\text{мест}\,i}$.
2. Размещение всех $N_{\text{СОИИ}}$ во всех $\sum_{i=1}^{L} N_{\text{мест}\,i}$ не влечет нарушения технологических и бизнес-процессов организации.
3. Отсутствие удаленных частей организации с каналами связи, по которым циркулирует инсайдерская информация.

По мнению автора, выполнение всех трех условий характерно для предприятий первого типа (как правило, небольших). Невыполнение хотя бы одного условия влечет идентификацию предприятия как предприятия второго либо третьего типов. Наличие третьего условия обусловлено относительной дороговизной сетевых средств защиты (особенно сертифицированных) и более разветвленной структурой процесса обработки инсайдерской информации со всеми вытекающими последствиями.

Следует отметить, что предложенный подход к построению графа сложности предприятия позволит наглядно увидеть все информационные потоки инсайдерской информации, оценить объем и частоту передаваемой инсайдерской информации для принятия решений по внедрению систем сетевой защиты, а также объективно оценить $C_{\text{СПИ}}$ конкретной организации.

2. Определение места подразделения противодействия инсайдерской деятельности в организационной структуре предприятия

Место подразделения информационной безопасности и проблема подчиненности обсуждаются достаточно давно. Следует отметить, что единого мнения в сообществе специалистов по данному вопросу нет, различные авторы [12] отстаивают часто противоположные точки зрения, приводя разумные аргументы. В рамках данной статьи рассматривается место и подчиненность только подразделения ПИД без учета остальных составляющих подразделения информационной безопасности, службы безопасности и т.д. Небольшие предприятия (ИП и т.д.), в которых функцию подразделения ПИД может выполнить один человек или небольшая группа лиц, также не рассматриваются в данной статье.

В настоящее время наиболее распространены следующие схемы организации подразделения ПИД.

1. Подчинение службе безопасности (экономической, собственной и т.д.). Одна из наиболее часто встречающихся схем. Недостатком является то, что если ПИД осуществляется преимущественно программно-техническими методами, то данный функционал слабо пересекается со службой безопасности, что часто приводит к недопониманиям между руководством службы безопасности и подразделением ПИД. Положительным является тот факт, что полномочия у службы безопасности, как правило, очень высокие, что существенно упрощает работу подразделения ПИД.

2. Подчинение подразделению информационных технологий (ИТ). В данной схеме налицо конфликт интересов, поскольку работа подразделения ПИД подразумевает в том числе контроль исполнения сотрудниками ИТ-подразделения правил, предписаний и регламентов. Кроме того, значительная часть функций подразделения ИТ не совсем коррелируется с деятельностью подразделения ПИД. Достоинством является то, что подразделению ПИД значительно проще внедрять программно-технические системы.

3. Создание самостоятельного подразделения. Данная схема требует существенных финансовых издержек, обладает достоинствами первой схемы (подчиненности службе безопасности) и лишена недостатков второй схемы.

Поскольку основополагающим критерием оценки решений для подавляющего большинства руководителей предприятий является экономическая целесообразность, то предлагается следующая схема определения места подразделения ПИД (рис. 2).

Указанная схема не является единственно возможной, но позволяет аргументированно принимать решение о месте подразделения ПИД преимущественно с точки зрения экономической целесообразности.

Очевидно, что для предприятий первого и второго типа схема циркуляции инсайдерской информации минимизируется и может быть защищена в основном организационно-техническими мерами, управление которыми находится, как правило, в ведении службы безопасности.

В указанной схеме в случае трудоемкости в сфере ИТ, большей 50 %, предлагается создание отдельного подразделения ПИД, поскольку функции преимущественно не относятся к службе безопасности, а значительная трудоемкость приходится на ИТ. Включение подразделения ПИД в подразделение ИТ не даст существенного эффекта, но приведет к недостаткам второй схемы.

Рис. 2. Схема определения места подразделения ПИД

При трудоемкости подразделения ПИД в сфере ИТ, меньшей 50 %, возможны следующие варианты в порядке предпочтения:

- включение подразделения ПИД в службу безопасности, поскольку функций ИТ не очень много;
- создание обособленного подразделения ПИД.

По мнению автора, предлагаемая схема отражает основные тенденции подчиненности подразделения ПИД. Отсутствие на рис. 2 подчиненности подразделения ПИД подразделению ИТ объясняется чрезмерными рисками конфликта интересов и отсутствием в том числе существенного экономического эффекта. Для большой и малой трудоемкости ИТ по противодействию инсайдерской деятельности нет существенного экономического эффекта по следующим причинам: большая трудоемкость потребует значительных ресурсов параллельно классическим функциям ИТ, а малая приведет к наличию в ИТ-подразделении значительного штата сотрудников с другими функциями.

3. Определение ценности инсайдерской информации

Далее рассмотрим возможные подходы к оценке ценности инсайдерской информации, например, для создания реестра инсайдерской информации.

Под ценностью инсайдерской информации, как правило, понимается широкий круг свойств информации, которые определяют степень влияния и воздействия на деятельность организации в случае ее утечки к организации-конкуренту. Если информация касается незначительных вопросов и утечка такой информации не ведет к значительному ущербу, то фактом утечки такой информации можно в определенной мере пренебречь. В то же время информация о ситуации, которая чревата банкротством организации, требует повышенного внимания и привлечения значительных ресурсов даже в том случае, если риск маловероятен.

Несмотря на то что ценность инсайдерской информации включает в себя комплекс показателей, главным критерием значимости является потенциальный ущерб для организации, измеряемый в натуральных или денежных показателях.

Ценность инсайдерской информации может быть ранжирована в соот-

ветствии с определенным заданным критерием. Как правило, им является уровень потенциальных негативных эффектов для организации. Рейтинг может присваиваться как самой инсайдерской информации, так и ее источникам [13]. Для оценки ценности инсайдерской информации может быть применена шкала, представленная в табл. 1.

Представленная шкала не претендует на истину в последней инстанции, но, по мнению автора, может успешно применяться для ранжирования ценности инсайдерской информации (например, в реестре инсайдерской информации организации). Наиболее очевидным для ранжирования ценности инсайдерской информации и вероятности ее утечки в соответствии с табл. 1 является использование экспертного оценивания. Однако для оценки выполнения критерия $C_{\text{СПИ}} < C_{\text{риск}}$, кроме ранжирования, необходима стоимостная оценка инсайдерской информации. Следует отметить, что не всю инсайдерскую информацию можно достаточно легко оценить в денежном выражении (например, репутационный ущерб и т.д.). В этом случае, по мнению автора, целесообразно воспользоваться методом непосредственной оценки (балльным методом). Он позволяет определить, насколько один фактор более значим, чем другие. В этом случае диапазон изменения характеристик объекта разбивается на отдельные интервалы, каждому из которых приписывается определенная оценка (балл), например, от 0 до 10. Следует отметить,

Таблица 1

Шкала оценки ценности инсайдерской информации

Рейтинг	Оценка инсайдерской информации	Вероятность утечки	Последствия утечки для организации
5	Имеет решающее значение для деятельности организации	Высокая	Катастрофические
		Средняя	
		Низкая	
4	Высокая значимость	Высокая	Значительные
		Средняя	
		Низкая	
3	Средняя значимость	Высокая	Умеренные
		Средняя	
		Низкая	
2	Низкая значимость	Высокая	Малозначительные
		Средняя	
		Низкая	
1	Незначительный риск	Высокая	Несущественные
		Средняя	
		Низкая	

что экспертное оценивание не является темой данной статьи, поэтому определение степени согласованности мнений экспертов и другие вопросы оценки адекватности и качества экспертного оценивания выходят за рамки данного материала.

Для определения стоимости инсайдерской информации (на основе полученных балльных оценок) можно воспользоваться аддитивной моделью. При использовании данной модели определение ценности базируется на экспертных оценках компонентов данной информации, и при объективности стоимостных оценок ее компонентов подсчитывается искомая величина — их сумма в стоимостном эквиваленте [13]. Основная проблема заключается в том, что количественная оценка компонентов информации часто оценивается необъективно, даже если оценка выполняется высококвалифицированными специалистами, причина заключается в неоднородности компоненов в целом. Для решения этой проблемы принято использовать иерархическую относительную шкалу, которая представляет собой линейный порядок, с помощью которого сравниваются отдельные компоненты по ценности один относительно другого. Случай единой шкалы равносилен тому, что все компоненты, имеющие равную порядковую оценку, равноценны.

Рассмотрим следующий пример. Пусть даны n объектов инсайдерской информации O_1, O_2, ..., O_n, оценка проводится по десятибалльной шкале; результат оценки экспертами — вектор ценностей объектов каждого относительно другого: (3, 5, ..., 8). Предположим, что изначально определена цена одного из объектов, например $O_2 = 150$ тыс. руб.

Вычисляем стоимость одного балла: $O_2/k = 150/5 = 30$ тыс. руб., где k — оценка объекта в баллах.

Аналогичным образом выполняется оценка других объектов. Сумма стоимостей объектов инсайдерской информации дает полную стоимость всей инсайдерской информации.

Рассмотрим обратную ситуацию. Если известна конечная стоимость инсайдерской информации, то исходя из нее можно обратным преобразованием определить стоимость каждого объекта инсайдерской информации.

С учетом применения метода непосредственного оценивания и аддитивной модели табл. 1, например, принимает числовой вид, который можно с успехом применять для проверки критерия $C_{\text{СПИ}} < C_{\text{риск}}$.

Рассмотрим два подхода для оценки ценности инсайдерской информации с точки зрения ее пользы для организации-конкурента. Следует отметить, что при зеркальном рас-

смотрении (с позиции оценки инсайдерской информации организацией) данные подходы справедливы для определения $C_{риск}$.

Прагматичный подход к оценке информации (в нашем случае — инсайдерской информации) предложен А. А. Харкевичем [14, 15]. Мерой ценности информации является изменение вероятности достижения цели при получении этой информации. В нашем случае количественная мера ценности инсайдерской информации $I_ц$ выражена следующим образом:

$$I_ц = \log P_1 - \log P_0 = \log P_1/P_0,$$

где P_0 — начальная, до получения инсайдерской информации, вероятность достижения цели организацией-конкурентом; P_1 — вероятность достижения цели организацией-конкурентом после получения информации.

Возможны следующие три случая. В первом случае полученная инсайдерская информация является ценной, увеличивающей вероятность достижения цели организацией-конкурентом, т.е. $P_1 > P_0$. Следовательно, информация является ценной, полезной, и количественная мера ценности информации $I_ц > 0$.

Во втором случае информация не изменяет вероятность достижения цели организацией-конкурентом. Она является бесполезной. При этом $P_1 = P_0$ и $I_ц = 0$.

В третьем случае вероятность достижения цели уменьшается, поскольку полученная информация является ложной, ошибочной. При этом $P_1 < P_0$ и $I_ц < 0$.

Данный подход можно успешно применять совместно с методами экспертного оценивания, представленными ранее.

Рассмотрим подход, *основанный на изменении экономической эффективности принятых решений* организацией-конкурентом после получения инсайдерской информации.

Например, некоторая организация-конкурент является одним из лидеров отрасли. Ей необходимо провести модернизацию своих производственных мощностей. На рынке также имеется другая организация, которая в силу своей значительности обладает информацией о перспективах развития рынка. Данная информация, несомненно, представляет интерес для организации-конкурента, поскольку позволяет выработать оптимальную стратегию развития. Цель организации-конкурента — определить ценность инсайдерской информации организации.

Допустим, руководство организации-конкурента рассматривает три варианта действий:

- вложить средства в собственную разработку производственных мощностей на новом технологическом уровне, не имеющих аналогов у конкурентов;
- вложить средства в закупку имеющихся на рынке технологий;
- не проводить модернизацию производств (бездействие).

Размер выигрыша или потерь организации-конкурента зависит от благоприятного или неблагоприятного состояния рынка [16].

Первоначально информация о состоянии рынка отсутствует, но экономисты могут рассчитать выигрыши/потери организации-конкурента от реализации стратегий при благоприятных и неблагоприятных условиях. В соответствии с принципом Байеса состояние рынка (благоприятное или неблагоприятное) принимают равновероятным и равным 0,5.

Средний ожидаемый выигрыш рассчитывается по формуле:

$$W = P_б W_в + P_н W_п,$$

где $P_б$ и $P_н$ — вероятности благоприятных и неблагоприятных состояний соответственно; $W_в$ и $W_п$ — выигрыши и потери организации-конкурента соответственно.

Результаты расчетов до и после получения инсайдерской информации от организации представлены в табл. 2 и 3.

Результаты расчетов показывают, что наилучшим решением при отсутствии инсайдерской информации является закупка технологий, так как при этом средний выигрыш максимален и равен $W_0 = 10$ млн руб.

Допустим, покупка инсайдерской информации обойдется организации-конкуренту в 1 млн руб. Инсайдерская информация указы-

Таблица 2

Средний выигрыш до получения инсайдерской информации

№	Действия организации-конкурента	Выигрыш/потери в зависимости от конъюнктуры рынка		Средний выигрыш до получения инсайдерской информации
		Благоприятный $P_б = 0,5$	Неблагоприятный $P_н = 0,5$	
1	Собственная разработка	130 млн руб.	−120 млн руб.	5 млн руб.
2	Покупка технологий	30 млн руб.	−10 млн руб.	10 млн руб.
3	Бездействие	10 млн руб.	−20 млн руб.	−5 млн руб.

Таблица 3

Средний выигрыш после получения инсайдерской информации

№	Действия организации-конкурента	Выигрыш/потери в зависимости от конъюнктуры рынка		Средний выигрыш после получения инсайдерской информации
		Благоприятный $P_б = 0,7$	Неблагоприятный $P_н = 0,3$	
1	Собственная разработка	130 млн руб.	−120 млн руб.	55 млн руб.
2	Покупка технологий	30 млн руб..	−10 млн руб.	18 млн руб.
3	Бездействие	10 млн руб.	−20 млн руб.	1 млн руб.

вает на то, что прогнозируется благоприятное состояние рынка с вероятностью 0,7 и неблагоприятное с вероятностью 0,3. В этом случае максимальный средний выигрыш (W_1 = = 55 млн руб.) организация-конкурент получит при выборе стратегии по собственной разработке производственных мощностей на новом технологическом уровне.

Таким образом, полученная дополнительная информация изменяет представление о целесообразности стратегии организации-конкурента и, соответственно, изменяет экономический эффект с 10 млн руб. до 55 млн руб.

Ценность дополнительной информации равна разности максимальных средних выигрышей организации-конкурента до и после получения инсайдерской информации с учетом стоимости самой информации:

$$I_ц = (W_1 - W_0) - S_п,$$

где $S_п$ — стоимость получения инсайдерской информации.

Для рассмотренного примера $I_ц = (55 - 10) - 1 = 44$ млн руб.

Таким образом, ценность инсайдерской информации определяется выгодой от ее использования. Ценность инсайдерской информации может существенно превысить стоимость ее получения. Платить за инсайдерскую информацию имеет смысл, если $(W_1 - W_0) > S_п$, т. е. $I_ц > 0$.

В рассмотренном примере инсайдерская информация указывает на прогноз благоприятного и неблагоприятного состояния рынка, что на практике, например, можно определить по числу выпускаемых в продажу средств производства с определенными характеристиками, которые влияют на конкуренцию в определенном сегменте и объеме рынка.

Очевидно, что $I_ц$ входит в $C_{риск}$, а в некоторых случаях полностью тождественно $C_{риск}$.

Заключение

Предложенные подходы к оптимизации организационной структуры предприятия и определению места подразделения противодействия инсайдерской деятельности позволяют на интуитивно понятном уровне, используя здравый смысл, противодействовать инсайду. Развитие предложенных подходов позволит выявить схожие по характеристикам предприятия и объединить их в кластеры в целях повышения качества оценок, возможности оптимизации, а также повышения объективности и точности принятия решений.

Описанный экономический критерий целесообразности внедрения средств ПИД (взятый из классической теории информационной безопасности) во многих трудах незаслуженно отсутствует, что с точки зрения практической реализации некорректно ввиду его ключевой роли (например, для руководителей организации).

Рассмотренные подходы к внедрению средств ПИД для различных предприятий, по мнению автора, являются наиболее логичными и позволяют быстро определиться сквозь призму экономической целесообразности с методами, формами и средствами противодействия инсайдерской деятельности. Дальнейшими направлениями развития являются разработка типовых моделей предприятий с детализацией условий классификации и характеристик для сложных организаций.

Представленные подходы к оценке и ранжированию инсайдерской информации могут с успехом применяться на практике, поскольку достаточно просты и интуитивно понятны. Выбор используемого подхода должен определяться удобством и наличием исходных данных для конкретной организации.

Список литературы

1. **Жемчугов А. М., Жемчугов М. К.** Организационная структура и стратегия предприятия // Проблемы экономики и менеджмента. 2011. № 2.

2. **Шершнева З. Е.** Стратегическое управление. К.: КНЭУ, 2004. 394 с.

3. **Ахмедов Т. Ч.** Междисциплинарный подход к вопросу выявления недобросовестного инсайдера в организации // Вестник Московского университета МВД России. 2014. № 2.

4. **Карпычев В. Ю., Сычев В. М.** Применение байесовских сетей в задачах анализа внутренних угроз информационной безопасности // Вестник Воронежского института МВД России. 2015. № 1.

5. **Matthew L. Collins's, Randall F. Trzeciak** et al. Common Sense Guide to Mitigating Insider Threats, Fifth Edition. Software Engineering Institute Carnegie Mellon University. Technical Report. December 2016.

6. **Кабанов А. С., Лось А. Б.** Причины, профилактика и методы противодействия инсайдерской деятельности // Безопасность бизнеса. 2016. № 3.

7. **Кабанов А. С., Суроев А. В., Лось А. Б.** Методы социальной инженерии в сфере информационной безопасности и противодействие им // Российский следователь. 2015. № 18.

8. **Веденеев В. С., Бычков И. В.** Системы выявления инсайдеров // Математические структуры и моделирование. 2014. № 4(32).

9. **Сычев В. М.** Формализация модели внутреннего нарушителя информационной безопасности // Вестник МГТУ им. Н. Э. Баумана. 2015. № 2.

10. **Гайкович В. Ю., Ершов Д. В.** Основы безопасности информационных технологий. М.: МИФИ, 1995. 96 с.

11. **Наумов В. Н., Кучеренко Д. В.** Исследование структурной сложности инфраструктуры государственных информационных систем методами анализа социальных графов // Современные наукоемкие технологии. 2019. № 2. С. 114—122.

12. **Директор** по информационной безопасности // Государство. Бизнес. ИТ, 2017. URL: http://www.tadviser.ru/index.php/Статья:Директор_по_информационной_безопасности_(Chief_information_security_officer,_CISO).

13. **Шарамко М. М.** Внутренний контроль: методология, система и процессы. М.: Русайнс, 2016. 228 с.

14. **Грушо А. А., Тимонина Е. Е.** Теоретические основы защиты информации. М.: Яхсмен, 1996.

15. **Волкова В. Н.** Теория информационных процессов и систем: учебник и практикум для академического бакалавриата. М.: Издательство Юрайт, 2016. 502 с.

16. **Лазебник В. М.** Экономическая кибернетика. URL: https://studfiles.net/preview/1100363/.

A. S. Kabanov, Candidate of Science (PhD) in technology,
Associate Professor of the Department, e-mail: kabanov_as@mail.ru,
Moscow Institute of Electronics and Mathematics, National Research University
"Higher School of Economics", Moscow, 123458, Russian Federation

Optimization of the Organizational Structure of the Enterprise Taking into Account the Opposition of the Insider Activity

Various approaches to optimizing the organizational structure of the enterprise are considered and the relevance of this task in terms of protection from insider activity is substantiated. An algorithm is proposed for determining the location of the anti-insider unit in the organizational structure of the enterprise. A pragmatic approach to assessing the need and cost of introducing counter measures to insider activities is shown. The condition of economic feasibility of introducing means of counteracting insider activities is given, and approaches to assessing insider information are proposed and the main conclusions are formulated. The article is analytical in nature and may be useful to heads of information security services, teachers, graduate students and university students.

Keywords: *organizational structure of the enterprise, insider, insider activity, value of insider information*

DOI: 10.17587/it.26.222-230

References

1. **Zhemchugov A. M., Zhemchugov M. K.** Organizational structure and strategy of the enterprise, *Problems of Economics and Management*, 2011, no. 2.

2. **Shershneva Z. E.** Strategic management, Kyiv, National University of Economics, 2004, 394 p.

3. **Akhmedov T. Ch.** Interdisciplinary approach to the issue of identifying an unfair insider in an organization, *Bulletin of the Moscow University of the Ministry of internal Affairs of Russia,* 2014, no. 2.

4. **Karpychev V. Yu., Sychev V. M.** Application of Bayesian networks in the analysis of internal threats to information security, *Bulletin of the Voronezh Institute of the Ministry of internal Affairs of Russia*, 2015, no. 1.

5. **Collins's M. L., Trzeciak R. F.** et al. Common Sense Guide to Mitigating Insider Threats, Fifth Edition, Software Engineering Institute Of Carnegie Mellon University, Technical Report, December 2016.

6. **Kabanov A. S., Los A. B.** Reasons, prevention and methods of countering insider activity, *Business Security*, 2016, no. 3.

7. **Kabanov A. S., Suroev A. V., Los A. B.** Methods of social engineering in the field of information security and counteraction to them, *Russian Investigator*, 2015, no. 18.

8. **Vedeneev V. S., Bychkov I. V.** Systems for identifying insiders, *Mathematical Structures knd Modeling,* 2014, no. 4(32).

9. **Sychev V. M.** Formalization of the model of internal intruder information security, *Bulletin of the Bauman Moscow state technical University*, 2015, no. 2.

10. **Gaikovich V. Yu., Ershov D. V.** Fundamentals of information technology security, Moscow, Moscow Institute of engineering and physics, 1995, 96 p.

11. **Naumov V. N., Kucherenko D. V.** Study of the structural complexity of the infrastructure of state information systems by methods of analysis of social graphs, *Modern Science-Intensive Technologies*, 2019, no. 2, pp. 114—122.

12. **Chief** Information Security Officer, *State. Business. IT*, 2017, available at: http://www.tadviser.ru/index.php/Статья:Директор_по_информационной безопасности_(Chief_information_security_officer,_CISO).

13. **Shramko M. M.** Internal control: methodology, system, and processes, Moscow, Rusyns, 2016, 228 p.

14. **Grusho A. A., Timonina E. E.** Theoretical bases of information protection, Moscow, Jahsman, 1996.

15. **Volkova V. N.** Theory of information processes and systems: textbook and workshop for academic undergraduate studies, Moscow, Yurayt Publishing House, 2016, 502 p.

16. **Lazebnik V. M.** Economic Cybernetics, available at: https://studfiles.net/preview/1100363/.