Когда наука достигает какой-либо вершины,
с нее открывается обширная перспектива
дальнейшего пути.
С. И. Вавилов

Механізм регулювання економіки

УДК 004.05:338.4

Кавун С. В.

МОДЕЛЬ РАБОТЫ ИНСАЙДЕРОВ В ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

In the article the new approach to the problem of interior economic safety (ES) of enterprise activity is offered. It is grounded on the new model of insiders' operation in the enterprise activity and constructed on the basis of IDEFO standard. The comparative analysis of the statistical data − received during research − is also reduced.

Статья является продолжением статьи, опубликованной в журнале "Управління розвитком" №1(45) [1].

Целостное понимание функционирования любого субъекта предпринимательской деятельности невозможно без формализованного представления его экономической модели. Проведенный анализ [2] и предложенные методики [1] формируют входную информацию для создаваемой модели. Кроме того, были разработаны классификатор типов инсайдеров и классификатор их видов деятельности, которые позволяют использовать формализованный математический аппарат для построения модели работы инсайдеров. Ранее данная область описывалась лишь понятийным аппаратом и не позволяла описать деятельность инсайдеров в формализованном виде.

Целью статьи является формирование целостного представления в виде завершенной экономической модели работы инсайдеров в предпринимательской деятельности, построенной на основе статистического анализа данных и предложенных ранее методик автора [3].

Объектом исследования выступает система экономической безопасности (ЭБ) предпринимательской деятельности, построенная на базе различных методик управления [3].

Научная новизна − впервые сформирована полноценная формализованная модель работы инсайдеров на предприятии, построенная на основе международного стандарта методологии функционального моделирования IDEF0.

Модель работы инсайдеров в предпринимательской деятельности. Все инсайдеры работают по одним и тем же алгоритмам, отличие может зависеть только от специфики самого предприятия. В общем плане методику действий инсайдера можно представить в следующем виде:

1. *Выход на заинтересованную сторону, или, попросту, вербовка.*

На этом этапе значительную роль играют стимулы или причины заинтересованности или стремления организации взаимосвязи с фирмой-конкурентом, среди которых можно выделить:

недовольство суммой денежного вознаграждения (до 50%);

невостребованная инициатива (хуже всего, когда она еще и наказуема);

замедленный карьерный рост (более заметен на фоне другого сотрудника, проработавшего меньший срок и получившего повышение);

отторжение в коллективе;

совокупность случайных (это ключевое слово) ошибок, допущенных при выполнении своих обязанностей;

получение ложного обвинения за допущенные кем-то ошибки;

отрицательные черты характера.

Большинство (а может и все) данных фактов вполне может выявить, а следовательно, и предотвратить последствия достаточно подготовленный психолог, которого, кстати говоря, также необходимо должным образом стимулировать − это вознаграждение всегда окупится.

2. *Договоренность, или расстановка всех точек над "и".* Фирма-конкурент должна вынести достаточно обоснованное предложение − это, как правило, денежное вознаграждение или некоторое обязательство по обеспечению безопасного и обеспеченного существования инсайдера.

3. *Выбор.* Инсайдер должен провести сравнительный анализ положения дел на предприятии, где он работает, и предложения, выносимого фирмой-конкурентом, − выбрать оптимальный вариант.

4. *Выбор способа технической реализации.* На этом этапе инсайдер должен проработать используемые каналы утечки информации (данных), при их недостаточности (или недостаточности их возможностей) найти возможности и средства реализации нового канала. Также необходимо определиться с используемыми средствами (программными или аппаратными), изучить их возможности. Часто подобные средства предоставляются инсайдерам самими фирмами-конкурентами с подробными инструкциями по использованию.

5. *Определение места и времени реализации операции:* выявление оптимальных временных интервалов возможности доступа к необходимой информации, выяснение возможности использования имеющихся средств, моделирование процесса получения информации и возможности ее передачи по каналам утечки, выяснение прав и полномочий, расчет времени обнаружения утечки, составление схемы зачистки следов присутствия, формирование необходимого алиби или схемы ложного обвинения другого сотрудника. Этот этап характеризуется длительностью времени ожидания, что дает достаточно весомый шанс службе ЭБ провести контрмероприятия.

6. *Получение необходимой информации (данных).* Самый опасный для инсайдера этап, но и самый скоротечный во времени. Опасность заключается в возможности его задержания во время осуществления операции, что лишает его всякого алиби и возможности отвести обвинение. Именно этот этап дает 100-процентную гарантию выявления сотрудников данной категории без проведения различного рода расследований ГУИКБ [2]. Большую помощь в выявлении инсайдеров могут оказать:

введенная скрытая система видеонаблюдения (ее необходимость всегда можно обосновать даже с юридической точки зрения);

ведение журналов логирования (с обязательным их дублированием и резервированием);

использование дополнительных технических средств безопасности и защиты данных;

использование труда профессиональных сотрудников –администратора, сотрудников службы ЭБ, менеджеров и ряда других;

введение и контроль над выполнением требований и положений системы ЭБ предприятия.

7. *Выбор действий с полученной информацией (данными).* С ней можно осуществить следующие операции:

сразу "слить", используя выбранные (этап 4) каналы утечки;

оставить у себя (но это будет неоспоримым доказательством вины);

оставить на временное хранение в произвольном месте (до наступления благоприятного момента);

одуматься, предположить последствия и вернуть (уничтожить) либо незаметно, либо признаться в допущенной ошибке.

Периодическое проведение службой ЭБ предприятия аудита критической информации (данных) может ликвидировать (частично) выполнение операций на данном этапе.

Таким образом, из приведенного описания методики работы инсайдера можно сделать следующие выводы:

1. Никто не застрахован от возможности появления сотрудников данной категории.

2. Введение на предприятии профессионального психолога может оказать значительную помощь в предотвращении, а впоследствии и в выявлении инсайдеров, кроме того, этот шаг всегда финансово оправдан.

3. Если психолог в состоянии устранить лишь некоторые этапы действий инсайдера, то для ликвидации оставшихся этапов необходима организация службы ЭБ предпринимательской деятельности, основной первичной задачей которой является разработка и внедрение политики ЭБ.

Полученная на основе изложенной методики действий схема работы инсайдера на предприятии в графическом виде выглядит, как показано на рис. 1.

В подтверждении данных выводов можно привести еще одну статистику [3]: практически каждая пятая компания (19%) считает, что на долю инсайдеров приходится свыше 60% всего ущерба от угроз информационной и экономической безопасности (ИЭБ) [4], а 7% респондентов убеждены, что инсайдеры несут ответственность более чем за 80% всех потерь.

Рис. 1. **Схема работы инсайдера на предприятии**

Кроме того, свыше одной трети респондентов (39%) винят инсайдеров более чем в 20% всех своих потерь, вызванных реализацией угроз ИЭБ предпринимательской деятельности. Однако такой высокий уровень опасности не мешает подавляющему большинству предприятий (75%) замалчивать утечки и другие внутренние инциденты. Наконец, заключительный открытый вопрос показал, что наибольшей опасности ждут именно со стороны инсайдерских атак, то есть от утечек персональной и конфиденциальной информации.

Кроме того, одним из возможных вариантов решения данной проблемы, как было сказано выше, может быть привлечение настоящих специалистов-профессионалов. Однако все это составляет кадровый вопрос. В этом плане прогноз компании IDC весьма неблагоприятен: к 2008 году объем продаж в сегменте сетевых и информационных технологий вырастет по сравнению с нынешними показателями на 18%. К тому времени дефицит квалифицированных инженерных кадров, например, в Европе составит 0,5 млн. человек (примерно 1% от общей численности населения). В каждой третьей европейской стране спрос на инженеров в области ЭБ предпринимательской деятельности будет превосходить предложение более чем на 20%. Наиболее остро дефицит кадров скажется в государствах Восточной Европы, особенно не входящих в Евросоюз. В Украине нехватка таких специалистов достигнет 33,5%, в России – 24,5%, в то время как в Великобритании не превысит 9,3%. В абсолютном выражении дефицит кадров в России составит 60 тыс. человек, в Великобритании – 40 тыс., в Украине – 28 тыс.

По мнению аналитиков, нехватка специалистов с углубленным знанием сетевых технологий в таких областях, как IP-телефония, ЭБ и беспроводные сети, станет серьезным препятствием для внедрения новых разработок на предприятиях, тормозя экономический рост и снижая конкурентоспособность экономики. Кроме того, кадровый голод приведет к спекуляциям на рынке труда и подтолкнет к пересмотру системы мотивации сотрудников.

Исследование компании Deloitte в сфере ИЭБ показало, что 70% утечек обходятся средним финансовым институтам более чем в 1 млн. долларов каждая. Их исследования были опубликованы в итоговом отчете "2006 Global Security Survey".

Таким образом, на основе схемы работы инсайдера (см. рис. 1) получаем модель функционирования в стандарте IDEFO (рис. 2).

Рис. 2. **Модель работы инсайдера в организации**

Декомпозиция 1-го уровня модели работы инсайдера представлена на рис. 3, декомпозиция 2-го уровня – на рис. 4 – 5.

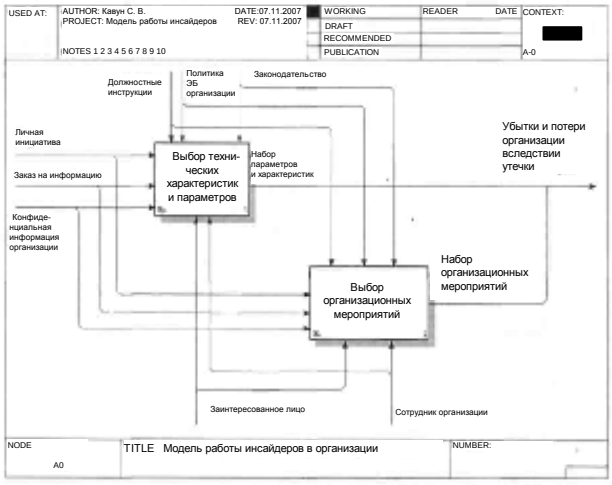


Рис. 3. **Декомпозиция 1-го уровня модели работы инсайдера**

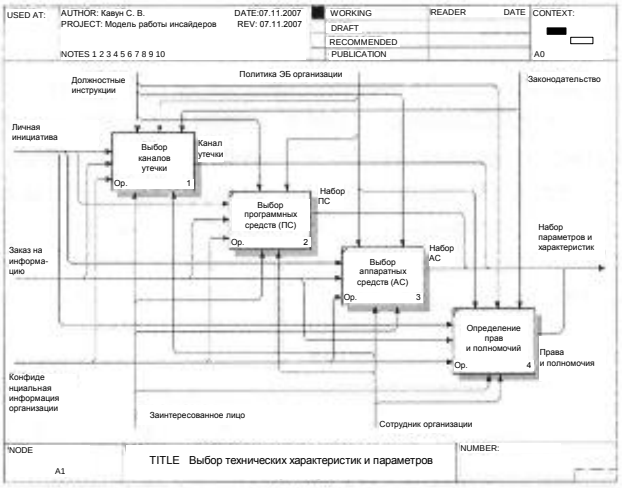


Рис. 4. **Декомпозиция 2-го уровня модели работы инсайдера (выбор технических характеристик и параметров)**

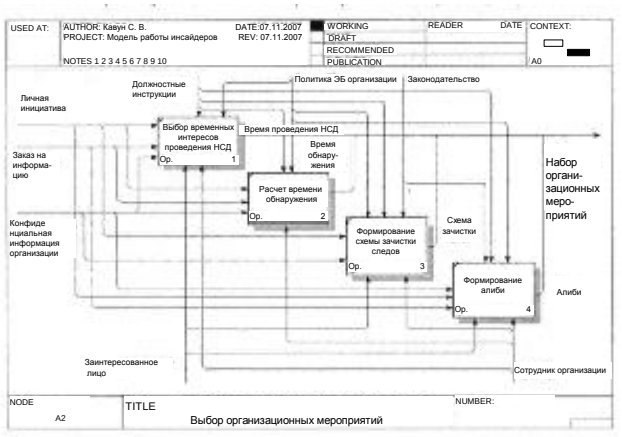
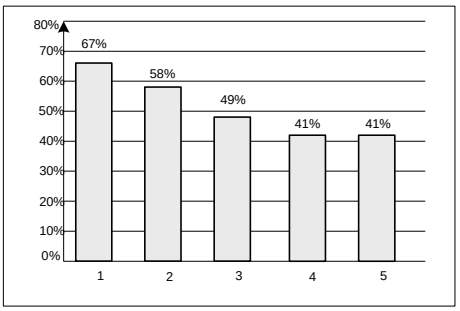


Рис. 5. **Декомпозиция 2-го уровня модели работы инсайдера (выбор организационных мероприятий)**

Можно проводить дальнейшую декомпозицию модели работы инсайдера до уровня конкретных операций и манипуляций, однако это приведет к неоправданному объему информации для дальнейшей обработки и анализа.

Все уровни модели работы инсайдеров в стандарте методологии функционального моделирования IDEFO представлены для получения последовательности и взаимосвязи действий инсайдера без учета их сложности и влияния на общий уровень системы ЭБ предприятия.

Для организации борьбы с проблемой инсайдеров необходимо, в первую очередь, выделить основные направления системы ЭБ в предпринимательской деятельности, в качестве которых по результатам компании Deloitte можно использовать приведенные на рис. 6.

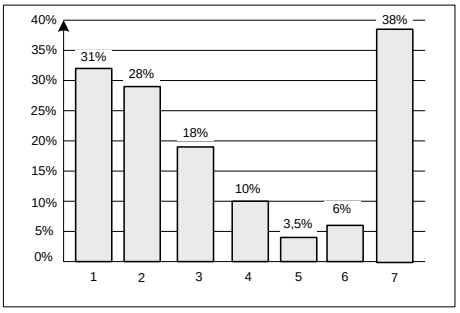


Условные обозначения:
1 – поддержка и совместимость с международными стандартами;
2 – защита от мошенничества с электронными счетами;
3 – непрерывное ведение бизнеса;
4 – процесс улучшения собственной инфраструктуры;
5 – использование управления идентификацией.

Рис. 6. **Основные направления функционирования системы ЭБ**

Рекомендуемые направления не являются стандартом или законом, это всего лишь рекомендации, полученные на основе анализа статистического исследования. Однако они есть справедливыми для всех предприятии, имеющих в своем активе финансовые отношения.

Каковы же основные воздействия на систему ЭБ предпринимательской деятельности со стороны инсайдеров? Можно выделить следующую классификацию типов воздействий, полученную на основе статистического анализа данных опроса. Результат представлен на рис. 7.



Условные обозначения:
1 – занесение вирусов;
2 – мошенничество;
3 – утечка категорированной информации о клиентах;
4 – компрометация корпоративной компьютерной сети;
5 – инциденты в беспроводных сетях Wi-Fi, WiMAX, Bluetooth, IrDA);
6 – другие различные формы компьютерных инцидентов;
7 – отвергают факты возникновения компьютерных инцидентов.

Рис. 7. **Классификация типов воздействий со стороны инсайдеров**

При расчете утечек всегда учитывают внутренние и внешние потери, у 2% опрошенных предприятий общий ущерб превысил 5 млн. долларов. Выводом данного исследования может быть выделение наиболее чувствительных к финансовым потерям предприятий, среди которых на первом месте находятся банки, страховые компании, корпорации, холдинги, предприятия с зарубежной долей инвестиций.

Таким образом, зная виды деятельности и классификацию типов воздействий инсайдеров, можно разработать комплекс мероприятий (методику), направленный на предотвращение или устранение последствий и результатов деятельности данной категории сотрудников.

В качестве основных видов деятельности в методике противоборства с инсайдерами можно рекомендовать использование следующих аспектов, представленных в таблице.

Таблица

Ключевые аспекты методики противоборства с инсайдерами

Для предотвращения	
1	2
1. Наблюдение, но не за сотрудниками (данное действие может быть воспринято как нарушение свободы личности), а за территорией пред приятия или за материальным имуществом, собственником которого как раз и выступает предприятие и с помощью которого (или за которым) выполняют свои обязанности сотрудники. При этом наблюдение может быть скрытым или открытым с записью и сохранением на внешних носителях, что потом может быть использовано в расследованиях ГУИКБ	2. Контроль использования ресурсов ИС предприятия (в личных, служебных, корпоративных и других целях). В основном для этих целей подходит использование электронных средств, но их использование для несанкционированного снятия информации запрещено законодательно [5, ст. 362, п. 2]. Однако использование компьютерных средств для мониторинга или аудита в системе ЭБ или администрирования законодательно не запрещено
3. Проведение мастер-классов, тренингов, семинаров, практических занятий с разъяснительной целью и построенное методически грамотно всегда наложит свой отпечаток и создаст предпосылки для предотвращения личной халатности сотрудников (доля которых составляет 42% от всего объема нарушений)	4. Периодический плановый мониторинг деятельности персонала предприятия. Его можно осуществлять в различных формах, например, ежемесячный личный отчет о своей деятельности перед непосредственным руководством в письменной форме. Подобный метод довольно широко используется в практике зарубежных компаний
Для выявления	
1. Использование распределенной системы мониторинга, автоматических средств аудита доступа (например, групп с ограниченным доступом – Restricted groups)	2. Организационные мероприятия, проводимые своевременно и аккуратно, позволят сократить, а может и ликвидировать долю операционных ошибок, которая составляет до 37%
3. Использование внешних источников информации, подчиненных службе ЭБ предприятия	

Окончание таблицы

1	2
Для ликвидации последствий	
1. Использование системы резервирования, что позволит своевременно и без больших затрат восстановить утраченную информацию	2. Использование систем физического разграничения доступа, особенно эффективны электронные средства слежения за внешними носителями, контроля использования портов компьютеров
3. Ограничение связи между внутренней корпоративной сетью и внешними сетями	4. Использование комплексных решений в области ЭБ предпринимательской деятельности, что позволит применить весь эффективный комплекс решений по обеспечению защиты, выявления и предотвращения возникновения подобных ситуаций

Однако, несмотря на все известные случаи, неоднократные публикации, явные предпосылки возникновения различных видов деятельности инсайдеров многие предприятия (28%) никак не фиксируют, а тем более не проводят расследования случившихся инцидентов.

Это, естественно, никак нельзя назвать эффективной практикой по реализации системы ЭБ на предприятии и, таким образом, это является своего рода поощрением несанкционированных действий инсайдеров. Кроме того, многие сотрудники реально представляют всю ценность каждой категории информации и, следовательно, могут воспользоваться фактом отсутствия выявления инцидентов.

Не стоит забывать, что даже элементарная единственная утечка информации может навсегда прекратить деятельность предприятия и привести его, например, к банкротству.

Таким образом, проблема внутренней ЭБ предпринимательской деятельности должна занимать достойное место в плане развития предпринимательской деятельности и получать все необходимые ресурсы (человеческие, организационные, финансовые и др.) для внедрения, реализации и соблюдения требований системы ЭБ предпринимательской деятельности.

В качестве предлагаемого направления дальнейшего исследования можно предложить разработку математической интерпретации задачи выявления (обнаружения) инсайдеров на предприятии, а также проведения анализа экономического эффекта использования предлагаемой модели и возможных последствий действий инсайдеров.

Литература: 1. Кавун С. В. Организация противодействия инсайдеров в предпринимательской деятельности // Економіка розвитку. – 2008. – № 1(45). – С. 9 – 11. 2. FBI. Compyter Crime Surver. Электронный ресурс FBI // http://houston.fbi/gov/pressrel/2006/ho011906.htm. 3. Кавун С. Методика построения политики безопасности организации / С. Кавун, Г. Шубина // Бизнес Информ. – 2005. – №1 – 2. – С. 96 – 102. 4. Кавун С. В. Информационная безопасность в бизнесе. – Харьков: Изд. ХНЭУ, 2007. – 408 с. 5. Кримінальний кодекс України // Відомості Верховної Ради (ВВР). – 2001. – №25 – 26. – С. 131.

Стаття надійшла до редакції 24.03.2008 р.