Розділ 3

Моделі та технології обробки фінансової інформації

УДК 33.338

Сорбат И.В.
Кавун С.В.

КОРПОРАТИВНЫЙ ИНФОРМАЦИОННЫЙ ПОРТАЛ – ИНСТРУМЕНТ БОРЬБЫ С ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТЬЮ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Аннотация. В статье раскрываются научные аспекты экономической безопасности предприятия, проводится исследование корпоративного информационного портала для комплексного решения прогнозирования, выявления и предотвращения инсайдерской деятельности. Сделаны выводы и рекомендации.

Ключевые слова: Экономическая безопасность предприятия, инсайдерская информация, инсайдерская деятельность, корпоративный информационный портал.

Введение. Экономическая безопасность предприятия (ЭБП) — это защита экономических интересов от внешних и внутренних угроз, что характеризуется совокупностью качественных и количественных показателей, целью которой является предостережение возможным утратам, угрозам банкротства предприятия [1].

Проблемы экономической безопасности предприятия приходится решать не только в период кризиса, но и при работе в стабильной экономической среде.

На сегодняшний день к причинам нарушения стабильной деятельности предприятия отнесли внутренние угрозы, такие как мошенничество, недобросовестная конкуренция, умышленные и неумышленные утечки конфиденциальной информации и интеллектуальной собственности (инсайдерская деятельность), а стихийные бедствия отступили на задний план.

Инсайдер (англ. Insider) – сотрудник, деятельность которого изменяется во времени под влиянием внешних и внутренних факторов и свойств индивида, а также его действий, которые в его социально-культурной среде могут быть расценены, как нарушение существующих норм (разглашение, подмена, уничтожение информации с ограниченным доступом) и традиций (не выполнения должностных обязанностей, норм корпоративной этики), и самого поведения, которое нарушает эти нормы (Кавун С. В.).

Инсайдерская информация (ИИ) – (англ. Insider information) – значимая и публично нераскрытая служебная информация компании, которая в случае ее

раскрытия существенным образом негативно влияет на функционирование компании (потеря конкурентоспособности, банкротство, рейдерский захват, нелегальная реэмиссия акций или активов и др.). Сотрудники, обладающие ИИ, как правило, являются доверенными лицами. Сотрудники, которые придали огласке ИИ, называются инсайдерами. Все это относится к сфере экономической безопасности, и составляет часть категориального аппарата (Сорбат И. В.).

В следствии возникает актуальность решения задачи организации системы экономической безопасности предприятия с целью предотвращения инсайдерской деятельности или сведения такой деятельности к мнимому. Над проблемами в данной сфере работают известные специалисты и ученые: Верин В.П., Гуров М.П., Олейников Е. А., Кизим М.О., Клебанова Т.С., Шкарлет С.Н., Кавун С.В. и др. [2-7]. Не до конца решенным остается вопрос внутренних угроз, и, как следствие, вопрос выявления (обнаружения) инсайдеров для предотвращения их деятельности.

Постановка задачи. Целью статьи является задача формализации практического применения корпоративного информационного портала на отечественных и зарубежных предприятиях как инструмента борьбы с инсайдерской деятельностью в системе экономической безопасности предприятия (ЭБП).

Результаты. Авторами статьи проведено исследование по фактам утечки информации, основанное на данных мировой статистики, которые были опубликованы в средствах массовой информации, веб-форумах, отчетов аналитических компаний, тематических блогах и других открытых ресурсах. В табл. 1 приведены статистические данные фактов умышленных и случайных утечек информации за определенный период времени во всем мире.

Таблица 1

Данные по видам утечек информации за определенный период времени

№	Вид утечек	2010		2009		2008		2007	
		Кол-во	%	Кол-во	%	Кол-во	%	Кол-во	%
1	Умышленные	402	48,0	375	51,0	241	45,5	154	29
2	Случайные	390	46,4	320	43,5	223	42,1	376	71
3	Не установлено	47	5,6	40	5,4	66	12,5	-	-

На рис. 1 представлена динамика утечек информации за заданный период времени, построенная на основе рассчитанных данных (табл. 1). Также были рассчитаны трендовые зависимости на основе полиномиальных зависимостей и их значения достоверности (R^2), по которым возможно получение дальнейших прогнозов.

Снижение количества случайных утечек информации за 2011 год по сравнению с предыдущим обусловлено тем, что с каждым годом в организациях внедряются различные методы и аппаратно-программные комплексы для выявления утечек информации. В большей части эти методы и средства позволяют выявить уже совершенные действия инсайдеров, но не спрогнозировать и предотвратить их.

Для дальнейшего исследования авторами предлагается комплексное решение, в основу которого входит использование корпоративного информационного портала на предприятиях как инструмента прогнозирования, выявления и предотвращения инсайдерской деятельности.

Корпоративный портал – это программный комплекс, который обеспечивает персонифицированный web-интерфейс, с помощью которого авторизированные сотрудники предприятия имеют доступ к необходимой информации и к дополнениям соответственно правам доступа. Это может быть не простой доступ сотрудника к

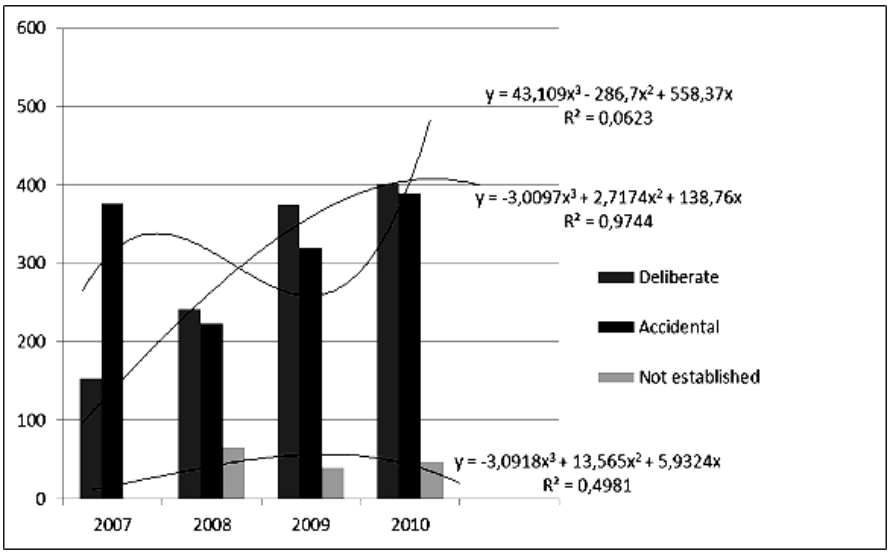

Рис. 1. Динамика утечек информации за заданный период времени

необходимой информации, это может быть организованный бизнес процесс, когда коллектив, территориально размещенных сотрудников, инструментами портала, решают единую задачу, которая имеет установленные ограничения по времени.

Сотрудник предприятия при использовании портала имеет следующий набор возможностей:

1) создавать шаблоны документов MS Office;
2) размещать и редактировать документы под общим доступом;
3) публиковать объявления о событиях;
4) задавать правила согласования документов;
5) отслеживать прохождение документов при согласовании;
6) формировать, размещать опрос и пересматривать результаты;
7) организовывать обсуждение;
8) использовать инструменты планирования – ставить задания, назначать события в календаре;
9) строить внешний вид портала в целом, так и для каждого сотрудника индивидуально;
10) разграничивать права доступа к документам и отслеживать их изменения.

Авторами, для предотвращения инсайдерской деятельности, предложена основа решения КИП в которой положены следующие функции:

1) доступ строго персонифицированный и регламентированный;
2) организация совместной удаленной работы сотрудников, когда каждый сотрудник находится за своим рабочим местом;
3) создание единой корпоративной базы данных как основа КИП;
4) взаимодействие на основе web-технологий, совместное редактирование общедоступных документов, а так же рабочее пространство для документов;
5) управление документами, которое позволяет сотруднику получать документы сразу из хранилища системы и управлять этими документами, модифицировать и и сохранять назад в хранилище новую версию;

КИП имеет следующие разделы: сотрудники, компания; библиотека документов, рабочие группы; календари событий, обучение; общения; фотогалереи; опроса.

Дополнительные возможности - инструменты для эффективной командной работы: система управления задачами и поручениями, организация встреч и собраний,

новые возможности календарей, обсуждение документов и документооборот [8].

Инструменты управления контентом: поиск, интеграция с офисными приложениями и календарями, подключения хранилищ документов, загрузки документов, хранение истории версий.

Реализован принцип единой системы авторизации. Активно используются инструменты социальной сети. Технические требования: портал интегрируется с Microsoft Office и Open Office, Active Directory и LDAP серверами, OpenID, работает на платформах UNIX и Windows (XP, Vista, Windows Server) поддерживает браузеры Internet Explorer и FireFox; Базы данных: MySQL, Oracle, MSSQL, MSSQL Express.

На уровне электронного документооборота:

– Описание бизнес-процессов предприятия с вложенными под процессами, поддержкой условий, циклов и т.д., включая графическое представление алгоритмов бизнес-процессов.

– Маршрутизация документов (WorkFlow), встроенные средства маршрутизации интегрированы с системами электронной почты, проведение изменений документации согласно ГОСТ 2.503-90.

– Использование корпоративных справочников при вводе в базу данных информации об объектах производства.

– Поддержка механизма версий объектов и документов, что позволяет хранить историю изменений; хранение документов как внутри базы данных, так и в файловой системе.

– Кроме того, система предоставляет большой набор функций, позволяющих специалистам предприятий самим создавать дополнительные программные модули.

Авторами статьи предлагается диаграмма последовательности потоков событий (рис. 2), описывающая поведение системы. Авторы обращают внимание на то, что диаграмма последовательности отображает поток событий для каждого варианта использования информации в КИП с целью выявления и предотвращения инсайдерской деятельности.

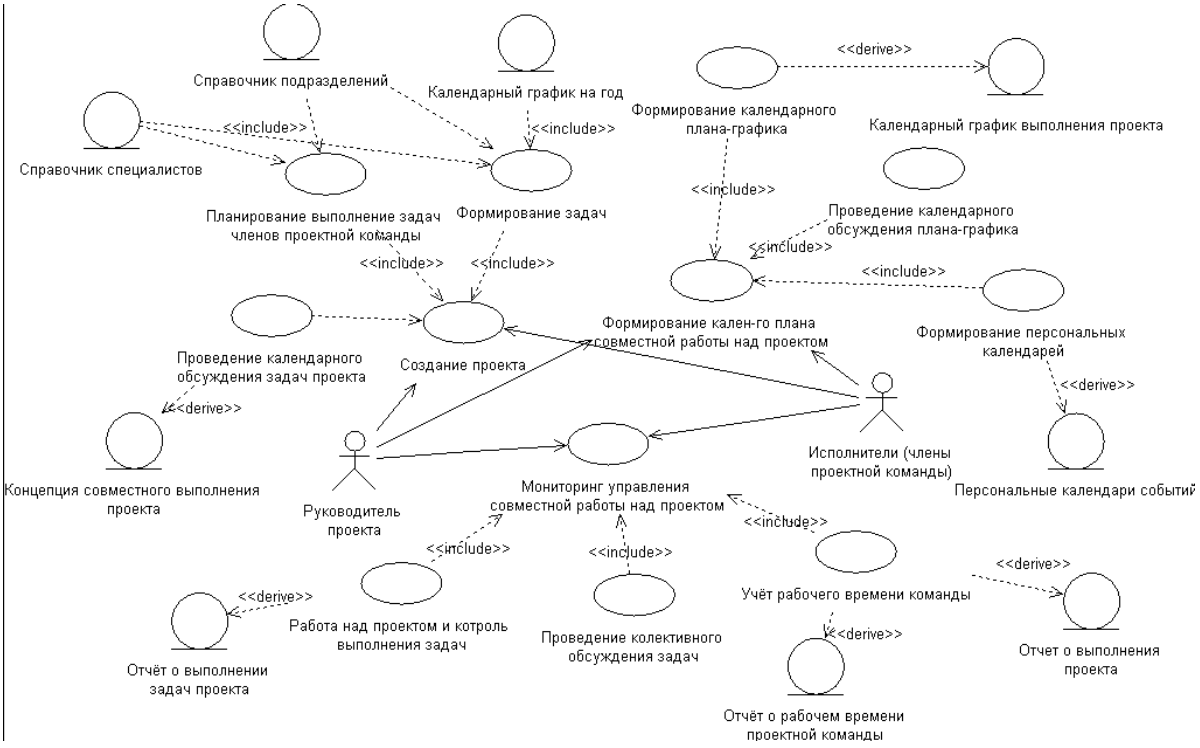

Рис. 2. Диаграмма последовательности потоков событий в КИП

Четкое управление информацией критично для успеха любой компании. Слабая организация управления информацией ведет к не эффективному взаимодействию, процессов принятия решений и потери потенциала в бизнесе. Предусмотренная авторизация сотрудников компании в КИП позволяет отслеживать время и дату обращения к информации, ее изменение в КИП и т.п., как один из механизмов вычисления инсайдерской деятельности с последующим выявлением инсайдера или группы инсайдеров. Рассмотрим некоторые примеры интерфейсного решения КИП. На рис. 3 представлен пример окна авторизации сотрудника КИП.

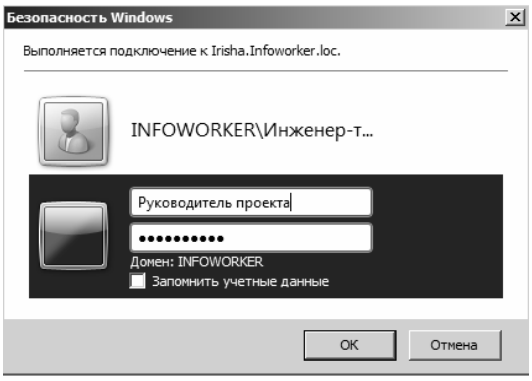

Рис. 3. Авторизация сотрудника КИП

На рис. 4 представлен список сотрудников имеющих доступ к конфиденциальной информации предприятия в КИП, где имеем возможность отследить наименование отдела, должность сотрудника, Ф.И.О. сотрудника, и др. данные.

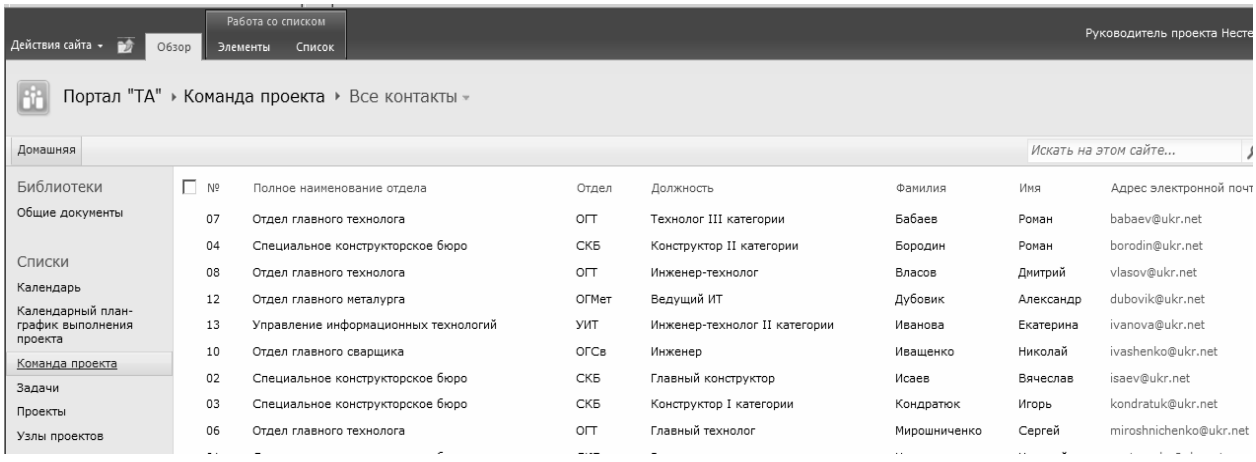

Рис. 4. Список сотрудников имеющих доступ к конфиденциальной информации предприятия

На рис. 5 представлено окно модуля контроля управления информацией портала, назначенные права доступа к информации, а так же сведения о времени и дате изменения информации сотрудником предприятия.

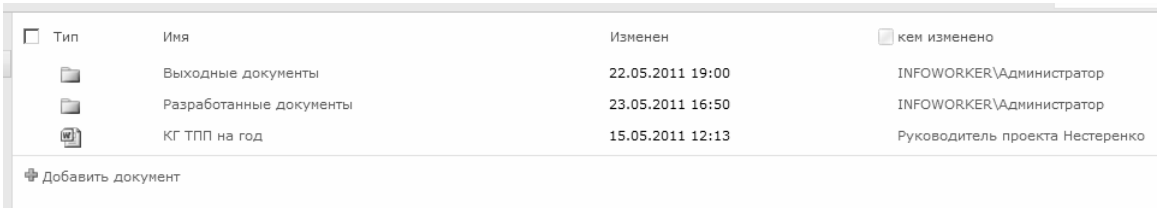

Рис. 5. Модуль контроля управления информацией портала

Таким образом, из результатов исследования, получим следующее, что функциональность корпоративного информационного портала покрывает решение нескольких основных задач предложенных авторами разделов положения о службе ЭБП:

1) разработка и осуществление профилактических мероприятий;
2) сбор, обработка, хранение и анализ официальной и конфиденциальной информации;
3) организация и проведение мероприятий по обеспечению безопасности персонала предприятия, основных фондов и финансовых активов;
4) проведение работ по обеспечению защиты информации;
5) внедрение нормативных актов по организации охраны помещений;
6) проведение единой технической политики в вопросах охраны;
7) контроль, выполнение требований службы ЭБП;
8) проведение инструктажа и обучения работников предприятия правилам работы с конфиденциальной информацией.
9) организация и осуществление совместно с отделами предприятия мероприятий по защите конфиденциальной информации;
10) проверка сведений, а также данных о попытках шантажа, провокаций и иных неблаговидных акций в отношении персонала;
11) взаимодействие с правоохранительными органами;
12) организация сбора, накопления, анализа и автоматизированного учета информации;
13) проведение проверок в подразделениях предприятия и оказание им практической помощи;
14) взаимодействие с другими подразделениями при осуществлении ими деятельности, связанной с иностранными специалистами;
15) внедрение положения о коммерческой тайне;
16) обучение работников банка практическим навыкам по обеспечению экономической, информационной и физической безопасности;
17) оказание содействия отделу кадров по работе с персоналом;
18) сбор, обработка, хранение, анализ информации о клиентах предприятия;
19) выполнение поручений руководства службы ЭБП.

Выводы. Предложенное авторами комплексное решение КИП, позволяет решить задачу прогнозирования, выявления и предотвращения инсайдерской деятельности. Так же по простой формуле можно рассчитать экономически более выгодное предложения по финансовым затратам предприятия на предложенное комплексное решение КИП. В отличие от сторонних решений, где используются специализированные программные средства по мониторингу сетей коммуникаций, не позволяющих спрогнозировать утечку информации и являющимися только как дополнительными решениями, которые необходимо периодически обслуживать и обновлять, что экономически не целесообразно для отечественных предприятий.

Литература

1. ES INFECO. Международный научно-исследовательский портал информационной и экономической безопасности // http://infeco.net.

2. Верин В.П., Преступления в сфере экономики. - М., Дело.2002.

3. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия // Управління розвитком. – 2008. – № 6. – С.17-21.

4. Кавун С.В., Сорбат И.В. Инсайдер – угроза экономической безопасности // Управління розвитком. – 2008. – № 6. – С.7-11.

5. Олейников Е. А. Экономическая и национальная безопасность: Учебник для вузов. – М.: Экзамен, 2005. – 768 с.

6. Геєць В. М. Моделювання економічної безпеки: держава, регіон, підприємство: Монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк.– Х.: ХНЕУ, 2006. – 240 с.

7. Гуров М.П., Кудрявцев Ю.А. Теневая экономика и экономическая преступность в вопросах и ответах: Учебное пособие. - СПб.: Санкт-Петербургский университет МВД России, 2002. - 237 с.

8. Михальчук І.В. Управління спільною роботою в умовах корпоративного інформаційного порталу. // Тези доповідей міжнародної науково-практичної конференції молодих вчених, аспірантів та студентів «Актуальні проблеми науки та освіти молоді: теорія, практика, сучасні рішення» «ІНЖЕК», 2011. – С. 145 – 146.

Summary. The article describes the scientific aspects of the economic security of the enterprise, conducted a study of corporate information portal for integrated solutions predict, detect and prevent insider trading activity. The conclusions and recommendations.

Keywords: Economic security of the enterprise, insider information, insider activity, enterprise information portal.

Стаття надійшла до редакції 12.03.2012