АЛЕКСЕЙ САФОНОВ,
руководитель группы проектов компании RCO

ЕВГЕНИЙ МАЛЬЦЕВ,
руководитель комитета МОО «АРСИБ» (Ассоциация руководителей служб информационной безопасности)

Ситуационно-аналитический Центр для компаний и банков

Представьте ситуацию – звонит разъяренный начальник и кричит в трубку, почему ему не докладывают о происшествии на объекте, а он вынужден узнавать об этом из местной прессы? А то и еще хуже – от высокопоставленного начальства, а уж те – из оппозиционного власти СМИ.

SHUTTERSTOCK.COM/WOWOMNOM

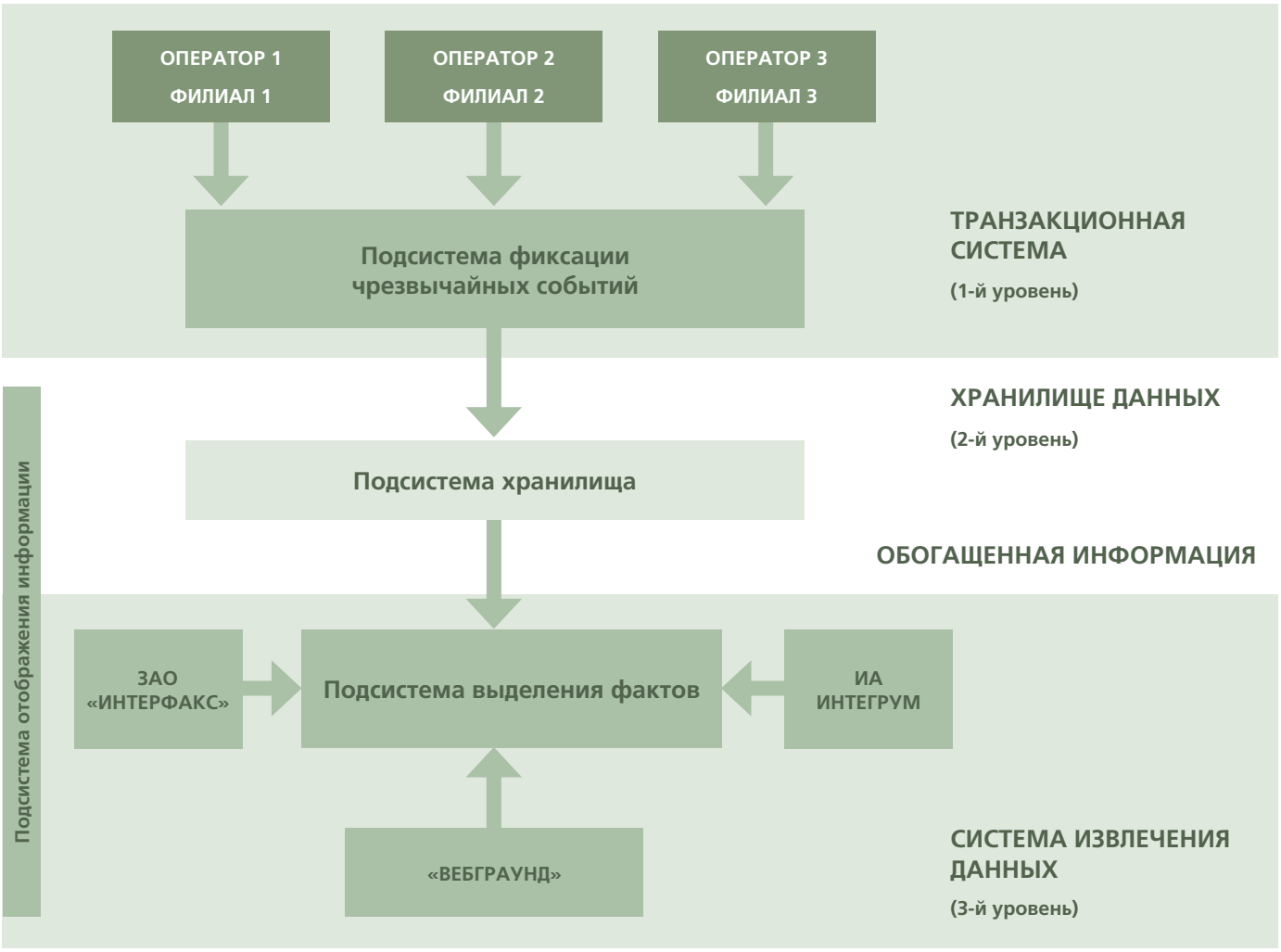
Не правда ли, вполне узнаваемая ситуация? Оставим за скобками те кары, которые сулит огорченное незнанием оперативной ситуации на производственных объектах руководство, и давайте задумаемся, как в реальной работе специалиста по безопасности избежать такого поворота событий? Особенно там, где на производстве много филиалов и соответственно, риски как возникновения чрезвычайного события на объекте, так и неполучения вовремя сообщения о нем возрастает многократно.

А следовательно, возрастают и угрозы возникновения репутационных рисков для предприятий и соответственно, рисков применения к руководителям СБ (на уровне начальников отделов) различных видов порицаний.

Конечно, важно своевременно получить информацию о чрезвычайном событии на вверенном вам объекте (будь то, например, обрушение крыши сборочного цеха на производстве в Ярославле, которое вызвало бурю публикаций сначала в соцсетях, а потом и в серьезных изданиях, таких как «Ведомости» и «Коммерсант», или, например, случай задымления в электричке от замыкания проводки светильника, как это было в вагоне, построенном известным машиностроительным холдингом). Эта информация сразу же может уйти дальше в «информационный океан», и, несомненно, распространение такой информационной «волны» вызовет новый виток усиления репутационных рисков.

Поэтому нужно не только вовремя получать информацию о случившемся, но и проводить работу по отслеживанию распространения ее в прессе и соцсетях – с фиксацией события в формализованном виде и дальнейшим насыщением карточки события информацией, позволяющей сопровождать ситуацию дальше в целях минимизации репутационных и коммерческих рисков, а также для сохранения информационного суверенитета компании.

Но, кроме фиксации события, необходимо также оценить масштабы бедствия с установлением материального ущерба, выявить и зафиксировать



возможных злоумышленников (или разгильдяев), по чьей вине произошел инцидент, при необходимости дособрать информацию о них из различных источников. Можно, например, уточнить, не является ли это лицо аффилированным с предприятием, фигурантом и т. д.).

Другими словами, накопленная информация должны быть собрана, систематизирована, загружена в единое хранилище данных с возможностью поиска похожих инцидентов, составления статистики по видам происшествий, филиалам, датам и тому подобное. Все это необходимо не как самоцель, а для разработки и проведения комплекса мероприятий по сокращению рисков и минимизации угроз компании.

А теперь представьте, что у вас в компании установлена (на вашем сервере) система, которая позволяет свести воедино все эти этапы работы с информацией, включив в общий информационный контур не только Центр и филиалы, но и различных специалистов из смежных с СБ направлений деятельности, которые пользуются единым для всего холдинга или банка информационным потоком.

Такая система могла бы состоять из 3-х уровней:

1-й уровень – подсистема фиксации чрезвычайных событий (на производстве/банке/компании, по всей филиальной сети) и работа с ними.

Если коротко, то специалист по безопасности или лицо, первым получившее информацию о событии (оператор ТСО, например), может зайти в систему удаленно из любого филиала через защищенный веб-интерфейс и сформировать карточку события, в которую вносятся первоначальные данные – вид инцидента (можно выбрать как из справочника, так и внести вручную), дату и время обнаружения, пострадавших, злоумышленников, предполагаемую сумму ущерба и т. д. Особое удобство – информация о появлении карточки события в системе отсылается должностному лицу, ответственному за это направление деятельности СБ, в виде сообщения электронной почты либо смс-сообщения.

После заведения карточки в системе с ней можно работать дальше – добавлять/убирать информацию согласно иерархии доступа, проводить дополнительный поиск информации как в открытых источниках («СПАРК», «Контур Фокус», «Интегрум», «Прима Информ», «КредитИнформ», и т. д.) так и во внутренних базах предприятия («Черные списки», «Реестры недобросовестных поставщиков», телефонные справочники

компании и т. д.), выгружать информацию из карточки для формирования досье и делать групповую выгрузку карточек для формирования статистики происшествий, а также многое другое. В том числе – присваивать категории конфиденциальности поступившей информации. При этом из филиалов не нужно «гонять» в центр электронные письма в ответ на каждое изменение ситуации по чрезвычайному событию – информацию можно вносить в режиме он-лайн сразу же по получению.

2-й уровень составляет подсистема интеграции базового хранилища карточек инцидентов с ведомственными системами оповещения о ЧП – например, с системой ЦППК (Центральной пригородной пассажирской компании), в которой фиксируют факты возникновения ЧП на железнодорожном транспорте.

Такого рода информацию можно как прикреплять к карточкам объектов или инцидентов, так и дальше производить по ней весь комплекс мероприятий работы – осуществлять дополнительный поиск в ручном режиме упоминаний инцидента в социальных сетях, в интернет-СМИ, в новостных лентах информационных агентств – для проведения оперативной работы по минимизации репутационных и иных видов рисков.

3-й уровень составляет подсистема выявления различных фактов (связанных с возможными предустановленными видами чрезвычайных событий) из потока неструктурированной информации, поставляемой различными компаниями-агрегаторами новостной информации, прежде всего ЗАО «Интерфакс» и ИА «Интегрум». Выделение фактов также доступно из потоков специализированных открытых источников, таких, как, например, проект «Вебграунд», поддерживаемый компанией RCO.

Факты по выбранной тематике и ключевым словам автоматически «заливаются» в карточку релевантного с ними инцидента/объекта, а также направляются в виде электронных или смс сообщений ответственным за это направление деятельности компании лицам. При этом из фактов могут выделяться даты, что позволяет в дальнейшей аналитической работе визуализировать их по временной шкале. Система также позволяет отмечать место и время появления этого факта на электронной карте.

Подсистема в режиме он-лайн мониторинга выявляет факты путем накладывания специально сконструированных лингвистических шаблонов (которые включают не только ключевые слова и словосочетания, как в обычных поисковых интернет запросах, но и связи между ними, а также учитывает их грамматические характеристики и семантические атрибуты). Уже сейчас библиотека из более чем 1000 шаблонов позволяет выявлять большое количество фактов, в том числе и об открытии новых производств, новых рынков, появления инноваций на рынке и т. д.

Можно воспользоваться поисковыми возможностями подсистемы и в ручном режиме, задав запрос с нужными ключевыми словами, в том числе можно искать фразы и использовать для точного поиска специальный язык запросов.

Кроме того, в библиотеке шаблонов есть такие, которые описывают еще не случившиеся событие – еще только планируемые участия в выставках и симпозиумах ваших партнеров и конкурентов, объявленных ключевыми лицами компаний, высказывания первых лиц компаний о закладках новых производственных мощностей или будущих вхождениях в бизнес-проекты, в том числе и на зарубежных рынках, и т. д. Эти «отловленные» анонсы событий могут служить инструментом информационного обеспечения выполнения задач совершенно новых для предприятия, например, для разработки реализации экспортной стратегии компании, обеспечивающей выход на совершенно новые для предприятия рынки.

Так что внедрение таких систем позволяет не только вовремя получать информацию о уже произошедших событиях, чтобы успеть «отработать» по ним и минимизировать различные виды рисков, но и выявлять информационные «кирпичики» знаний, позволяющие выстраивать «в будущее» стратегию успеха компании.

А как же банки, спросите Вы? Очень просто – из промышленного варианта такая система легко превращается в банковскую посредством смены справочников структуры организации, видов чрезвычайных событий, небольшой доработкой выводных форм и подключением к системе банковских и финансовых источников информации.

Принцип же фиксации и дальнейшей работы с сообщениями о ЧС остается прежним.

Комментирует Александр Корнеев, руководитель информационно-аналитического отдела Департамента безопасности ОАО «РЖД»

«Выявить каналы утечки ведомственных документов РЖД».

Не так давно моим руководством была поставлена задача – выявить и пресечь каналы распространения внутренних документов РЖД. Время от времени они появлялись на разных сайтах – то на одних, то на других, и затем нередко перепечатывались серьезными изданиями.

В результате проведенных работ мы вычислили эти каналы – оказалась, что «слив» шел через обычную с виду страничку ВКонтакте, и велся в «мерцающем режиме». Через некоторое время после опубликования документов, когда проходила перепечатка, документы изымались и страничка превращалась в обыкновенную.

И если бы в тот момент мы могли бы промониторить открытый Интернет, в том числе и социальные сети, по специальному шаблону, который можно создать в такой системе. Например, шаблон: ОАО «РЖД» (с различными видами написаний компании) + слова, обозначающие вид документа – «Приказ» или «Распоряжение» или «Инструкция») и т. д., и сделать это в автоматизированном режиме, то мы смогли бы отловить такой «слив» в самом начале сброса, гораздо быстрее, чем в ручном режиме. А в ручном нам пришлось затратить довольно много времени, чтобы «обезвредить» этот канал, но в результате задачу, поставленную руководством, выполнили». ●