Список использованных источников:

1. Большой экономический словарь. - М.: Институт новой экономики. А.Н. Азрилян. 1997.
2. ГОСТ Р 53092-2008. Системы менеджмента качества. Рекомендации по улучшению процессов в учреждениях здравоохранения. Москва: Стандартинформ, 2009. – 77 с.
3. О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года: Распоряжение Правительства РФ от 17 ноября 2008 г. № 1662-р // Собрание законодательства Российской Федерации. – 2008. - №47. – Ст. 5489.
4. О Стратегии национальной безопасности Российской Федерации до 2020 года: Указ Президента РФ от 12 мая 2009 г. № 537 // Российская газета – Федеральный выпуск. – 2009. – № 4912 (88), 19 мая 2009 г.

5. Перминов А.Ю., Фоменко Н.С. Методические аспекты формирования многомерной системы сбалансированных показателей // Бизнес. Образование. Право. Вестник Волгоградского института бизнеса. - 2012. - №3 (20). - С.69-72.

6. Рекомендации по стандартизации Р 50.1.028-2001. Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования. Москва: Госстандарт России, 2003. – 49 с.

7. Решетова Н.Э. Практика применения стандарта моделирования ЕРС [Электронный ресурс] – Режим доступа: <http://projectimo.ru/biznes-processy/notaciya-epc.html> (дата обращения: 07.03.2019).

Приложение 1**Форма модифицированной оперограммы**

№ п/п	Операция процесса	Участник 1	Участник 2	Участник 3	Частота	Кратность	Трудозатраты (в минутах)	Общее время за госпитализацию	Медикаменты				Расходные материалы				Оборудование, используемое в процессе			Помещения, используемые в процессе			Управление (стандарты, нормативные документы)
		А	Б	В					Наименование	Ед. измерения	Кол-во на манипуляцию	Кол-во на законченный случай	Наименование	Ед. измерения	Кол-во на манипуляцию	Кол-во на законченный случай	Наименование	Время использования за манипуляцию, мин	Время использования за законченный случай, мин	Наименование	Время использования за манипуляцию, мин	Время использования за законченный случай, мин	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРОМЫШЛЕННОМ ПРЕДПРИЯТИИ С ПОМОЩЬЮ РИСК – КОНТРОЛЛИНГА

Поникаров Владимир Александрович

Канд. техн. наук, профессор, кафедра проектного менеджмента, РТУ МИРЭА,

г. Москва;

Воронов Д.Г.,

к.э.н., доцент

Российского технологического университета МИРЭА, г. Москва

[DOI: 10.31618/ESU.2413-9335.2019.7.59.42-45](https://doi.org/10.31618/ESU.2413-9335.2019.7.59.42-45)

АННОТАЦИЯ: в статье обоснована необходимость обеспечения безопасности информационных ресурсов промышленных предприятий и использования для решения этой задачи риск-контроллинга (РК); рассмотрены вопросы, касающиеся определения понятия РК, его этапов, плана анализа службой РК влияния недостатков в обеспечении защиты информации на организационные риски промышленного предприятия.

ANNOTATION: the article substantiates the need to ensure the safety of information resources of industrial enterprises and use risk-controlling (RK) to solve this problem; The issues relating to the definition of the concept of the Republic of Kazakhstan, its stages, the plan for the analysis by the Service of the Republic of Kazakhstan of the influence of deficiencies in the protection of information on the organizational risks of an industrial enterprise were considered

Ключевые слова: безопасность информационных ресурсов, защита информации, контроллинг рисков, риск-контроллинг, служба риск-контроллинга.

Keywords: information resource security, information protection, risk controlling, risk controlling, risk controlling service.

Ни одно современное промышленное предприятие не может успешно работать на рынке без надлежащего информационного обеспечения, в тоже время рыночная среда отличается большой степенью неопределенности, носит вероятностный характер, поэтому любая деятельность предприятия (в том числе и его информационное обеспечение) подвержена широкому спектру рисков [1]. И действительно, российские промышленные предприятия постоянно сталкиваются с неординарными ситуациями, незапланированными или неординарными событиями, а это, в свою очередь, требует, с одной стороны, концентрации значительных объемов обобщенной и систематизированной информации, с другой - решения комплекса задач по обеспечению безопасности информационных ресурсов при одновременном сохранении максимальной их доступности для пользователей.

Под безопасностью информационных ресурсов обычно понимается их защищенность во времени и пространстве от любых, как объективных, так и субъективных по происхождению угроз, появляющихся как в обычных, так и в экстремальных условиях функционирования предприятия (стихийных бедствий, попыток конкурентов создать потенциальную или реальную угрозу несанкционированного доступа к базам данных и пр.).

По оценкам западных специалистов, утечка 20% информации, составляющей коммерческую тайну, в шести случаях из десяти приводит к банкротству даже самого преуспевающего предприятия, порой в течение нескольких суток. Для промышленных предприятий, которые для сохранения своих позиций на рынке, вынуждены непрерывно разрабатывать и внедрять новые образцы продукции, подобная опасность особенно велика. Опасность для информации производственного и экономического характера, которой обладает предприятие, может заключаться:

- в уничтожении этой информации;
- в ее несанкционированном получении и распространении лицами, не имеющими на это права;
- в ее целенаправленной модификации путем внесения искажающих ее изменений;
- во включении в базы данных ложных сведений;
- в отказе от включения в базы данных важных для предприятия сведений [2].

В результате возникает опасность разрыва деловых отношений с партнерами и клиентами и, как следствие из этого опасность: не заключения выгодных контрактов; отказа от решений, ставших неэффективными в результате разглашения конфиденциальной информации; использования конкурентами предприятия полученных сведений для повышения своей конкурентоспособности; нанесения ущерба авторитету предприятия и пр.

Результаты исследований причин нарушений говорят о том, что главный источник нарушений режима информационной безопасности находится внутри самого предприятия: 75- 85% нарушений совершаются его сотрудниками (пользователями, персоналом, обслуживающим технические средства, системными программистами, руководителями разных уровней), имеющими доступ к информационному обеспечению, и только 15-25% нарушений совершаются случайно или умышленно лицами со стороны [3].

Упомянутые нарушения могут повлечь за собой системный риск возникновения на предприятии кризисной ситуации. В качестве защиты от системного риска необходим инструмент, обеспечивающий координацию внутренних управленческих процессов, внешней и внутренней среды предприятия. В качестве такого инструмента может служить контроллинг рисков или риск-контроллинг (РК). Рассматривая контроллинг как систему управления, ориентированную на повышение эффективности работы предприятия, можно сформулировать определение РК предприятия, как процесс, состоящий в обеспечении определенного для данного предприятия соотношения между потенциальными возможностями достижения целей и угрозами негативных отклонений в результате реализации рискованных событий [4].

Учитывая зарубежные стандарты в области риск-менеджмента, можно выделить следующие этапы РК: определение целевого уровня рисков, идентификация и анализ рисков предприятия, оценка уровня риска, реализация мероприятий в отношении рисков, контроль выполнения запланированных мероприятий, учет и мониторинг [5].

Таким образом, с помощью РК можно создать систему управления защитой информации предприятия и контролировать источники рисков, вызванных ненадлежащим обеспечением этой защиты [6].

Прежде всего, от службы РК предприятия требуется хотя бы ориентировочно определить, какие риски наиболее вероятны и к каким потерям они

могут привести. Зная это, можно ответить на вопрос, как их уменьшить. Ответ этот должен включать перечень организационных мер профилактики рисков и программу их страхования.

Примерный план анализа службой РК влияния недостатков в обеспечении защиты информации на организационные риски промышленного предприятия представлен на рисунке 1. Этот процесс должен быть непрерывным, поскольку с внедрением новых видов информационных технологий и расширением своей функциональной деятельности возникают новые источники рисков.

Предпринимаемые меры по обеспечению защиты информации должны быть адекватны вероятности осуществления соответствующего типа угрозы и потенциальному ущербу, который может быть нанесен в том случае, если та осуществится (включая затраты на защиту от нее). Необходимо иметь в виду, что многие меры защиты требуют достаточно больших вычислительных ресурсов, что в

свою очередь существенно влияет на процесс обработки информации. В связи с этим современный подход к решению этой проблемы заключается в применении принципов ситуационного управления защищенностью информационных массивов.

Суть такого подхода заключается в том, что требуемый уровень безопасности информации устанавливается в соответствии с ситуацией, определяющей соотношение между ценностью перерабатываемой информации, затратами, которые необходимы для его достижения, и возможными суммарными потерями (материальными, моральными и др.) от искажения и несанкционированного использования информации. Выбирая защитные меры, приходится учитывать не только прямые расходы на закупку оборудования и программ, но и расходы на внедрение новинки и, в частности, на обучение и переподготовку персонала.

Рисунок 1 - План анализа службой риск-контроллинга влияния недостатков в обеспечении защиты информации.

Список литературы:

1. Завьялов Ф.Н., Кочерыгина Е.Е., Поникаров В.А. Совершенствование системы управления рисками деятельности промышленного предприятия: монография. - Ярославль: Издательство ООО «КопиЦентр», 2013. - 160 с.

2. Поникаров В.А., Ревенков П.В. Риск-контроллинг, как инструмент обеспечения безопасности информационных ресурсов предприятия // Материалы VI Международной научно-практической конференции «Фундаментальные и прикладные

проблемы приборостроения, информатики, экономики и права» в г. Сочи. - М.: МГАПИ, 2003. С. 128-134.

3. Ревенков П.В., Поникаров В.А. Методологические основы обеспечения информационной безопасности предприятия // Автоматизация и современные технологии. - № 3. - 2003. С. 29-34.

4. *Контроллинг: учебник / под редакцией А.М. Карминского, С.Г. Фалько.* - М.: Финансы и статистика, 2006. - 336 с.

5. Енгалычев О.В. Контроллинг рисков в деятельности промышленного предприятия // Вестник машиностроения. - № 1. - 2005. С. 35-40.

6. Поникаров В.А., Ревенков П.В. Обеспечение защиты информации предприятия на основе риск-контроллинга // Контроллинг. - № 3. - 2007. С. 3-9.