Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2017, № 1, с. 42-47.

Поступила: 02.09.2017
Окончательный вариант: 09.10.2017

© УлГУ

УДК 331.108

К вопросу информационного обеспечения кадровой безопасности организации

Подриз А. С.[1,2*]

[*]podriz_as@mail.ru
[1]УлГУ, Ульяновск, Россия
[2] НПО «Марс», Ульяновск, Россия

В статье рассмотрен подход к информационному обеспечению кадровой безопасности организации позволяющий уменьшить риски кадровой безопасности Определен порядок сбора и анализа информации о работнике с момента его приема на работу, заканчивая мероприятиями, проводимыми при увольнении. Подход основан на использовании структур данных, называемых профилями должности, личности, анализируя которые можно выявить у работника наличие склонностей к совершению определенных видов правонарушений, а также сделать предположения о его причастности к инцидентам безопасности.

Ключевые слова: *кадровая безопасность, информационное обеспечение, структуры данных*.

Введение

Современное предприятие можно представить как социотехническую систему, основными элементами которой являются следующие подсистемы: техническая, которая может включать в себя такие элементы как парк оборудования, материальные и финансовые ресурсы, информационные ресурсы, а также социальная, связанная с деятельностью персонала, управлением его вовлеченностью в достижение стратегических и краткосрочных целей организации, эффективностью труда и т.д. При этом основной целью функционирования такой системы является получение максимальной прибыли с наименьшими затратами ресурсов, т. е прирост ресурсов за счет деятельности, персонала в условиях воздействия внешней среды.

Персонал организации, являясь одним из важнейших элементов данной структуры, играет ведущую роль в достижении указанной цели. При этом действия или бездействие персонала в определенных ситуациях могут стать причинами реализации угроз безопасности организации. Проблемы противодействия угрозам, связанным с собственным персо-

налом организации, получают все большее внимание со стороны научного сообщества. Кадровая безопасность как самостоятельный аспект безопасности организации все чаще выделяется как в научной литературе, так и в нормативной документации различного уровня.

Целью настоящей работы является описание подхода к разработке информационного обеспечения кадровой безопасности организации. Задачами исследования являются анализ предметной области кадровой безопасности, а также описание процесса сбора структурированных наборов данных, необходимых для обеспечения кадровой безопасности организации.

Описание предлагаемого подхода

Обратимся к терминологии. Понятие «безопасность» определяется как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз[4]. В некоторых источниках, например в [2], безопасность определяется как отсутствие недопустимого риска. Данное определение на наш взгляд, является наиболее подходящим для формализованной постановки задач обеспечения кадровой безопасности.

Согласно [3] риск – это сочетание вероятности нанесения ущерба и тяжести этого ущерба. Под ущербом понимается нанесение физического повреждения или другого вреда здоровью людей, или вреда имуществу или окружающей среде.

Понятие кадровой безопасности можно определить как один из аспектов обеспечения безопасности организации, связанный с защитой от угроз, которые определены деятельностью юридических и физических лиц, специально направленной на нанесение конкретной организации имущественного или неимущественного ущерба, связанные с функционированием кадрового направления [5].

Кадровая безопасность занимает доминирующее положение в системе безопасности предприятия, так как непосредственным объектом воздействия подсистемы кадровой безопасности является персонал организации – определяющее звено в любом направлении деятельности, а человеческий фактор в большинстве случаев является основной причиной возникновения инцидентов безопасности предприятия.

Процесс обеспечения кадровой безопасности направлен на противодействие лишь определенным типам угроз. Классификация угроз кадровой безопасности [6] по объекту воздействия представлена на рис. 1.

Риски характеризуют опасность, которая может угрожать персоналу, имуществу компании. Мероприятия по минимизации рисков кадровой безопасности целесообразно проводить в отношении каждого сотрудника на этапе приема на работу (в том числе при прохождении испытательного срока), контроля за деятельностью в процессе работы. Кроме того, собранная информация позволит выработать комплекс мероприятий по минимизации рисков для компании при увольнении сотрудника.

Рис.1. Классификация угроз кадровой безопасности.

Для проведения указанных мероприятий подразделениям, непосредственно отвечающим за обеспечение кадровой безопасности (как правило, ими выступают кадровая служба и служба безопасности) требуется определенный набор информации о работнике (кандидате). Основными элементами в структуре информационных ресурсов, по нашему мнению, могут выступать взаимосвязанные наборы данных о работниках, связанных с компетенциями в организации и личностными особенностями каждого сотрудника. Указанные наборы данных будем называть профилями.

Для решения задач обеспечения кадровой безопасности предлагается формирование трех базовых профилей (см. схему на с. 47): профиля должности, профиля личности, профиля работника (агрегированные и дополненные данные из профиля должности и профиля личности).

Профиль должности представляет собой совокупность организационно-функциональных признаков должности (обязанностей, функций, реализуемых сотрудником в организации, отношения руководства и подчиненности), желательных требований к кандидату на замещение должности в части личных и деловых качеств, формальных аспектов, требований по оборудованию рабочего места, применяемых процедур внутреннего контроля, а также показателей эффективности работы [7]. Для целей обеспечения кадровой безопасности целесообразно включить в указанный профиль перечень угроз, реализация которых работником, замещающим должность, наиболее вероятна.

Формирование указанного профиля производится с использованием сведений из документированных источников (должностной инструкции, квалификационные справочники, профессиональные стандарты, локальные нормативные акты организации), а также профессиографических данных, на основе которых формируются рекомендации, связанные с психологическими и личностными особенностями кандидатов. Выбор перечня наи-

более вероятных угроз целесообразно проводить по специально алгоритмам, которые в настоящей статье не приводятся.

Профиль личности представляет собой совокупность данных о кандидате (работнике), претендующем на замещение какой-либо должности, включает в себя как биографические сведения о кандидате (работнике), так и данные, полученные на основании результатов изучения личности (психотип, темперамент и т.п), информации, полученной из социальных сетей и иных источников.

В соответствии с [1] проводить сбор указанной информации возможно только с письменного согласия кандидата (работника). Основываясь на этих данных, также можно сформировать перечень угроз безопасности организации, к которым имеется склонность у конкретного человека.

Объединяя данные из профиля должности и профиля личности, а также дополняя их, получаем так называемый профиль работника. Сведения из профиля работника позволят в дальнейшем определить перечень угроз, реализации которых может способствовать работник, объекты возможного ущерба, а также сформировать перечень инцидентов безопасности организации, к которым причастен конкретный работник. В дальнейшем эти данные дадут возможность количественно рассчитать риски реализации определенных видов угроз, связанных с деятельностью каждого работника, автоматически выработать как превентивные меры по недопущению реализации угроз, так и выработать меры реагирования на инциденты информационной безопасности, используя методы прецедентного анализа.

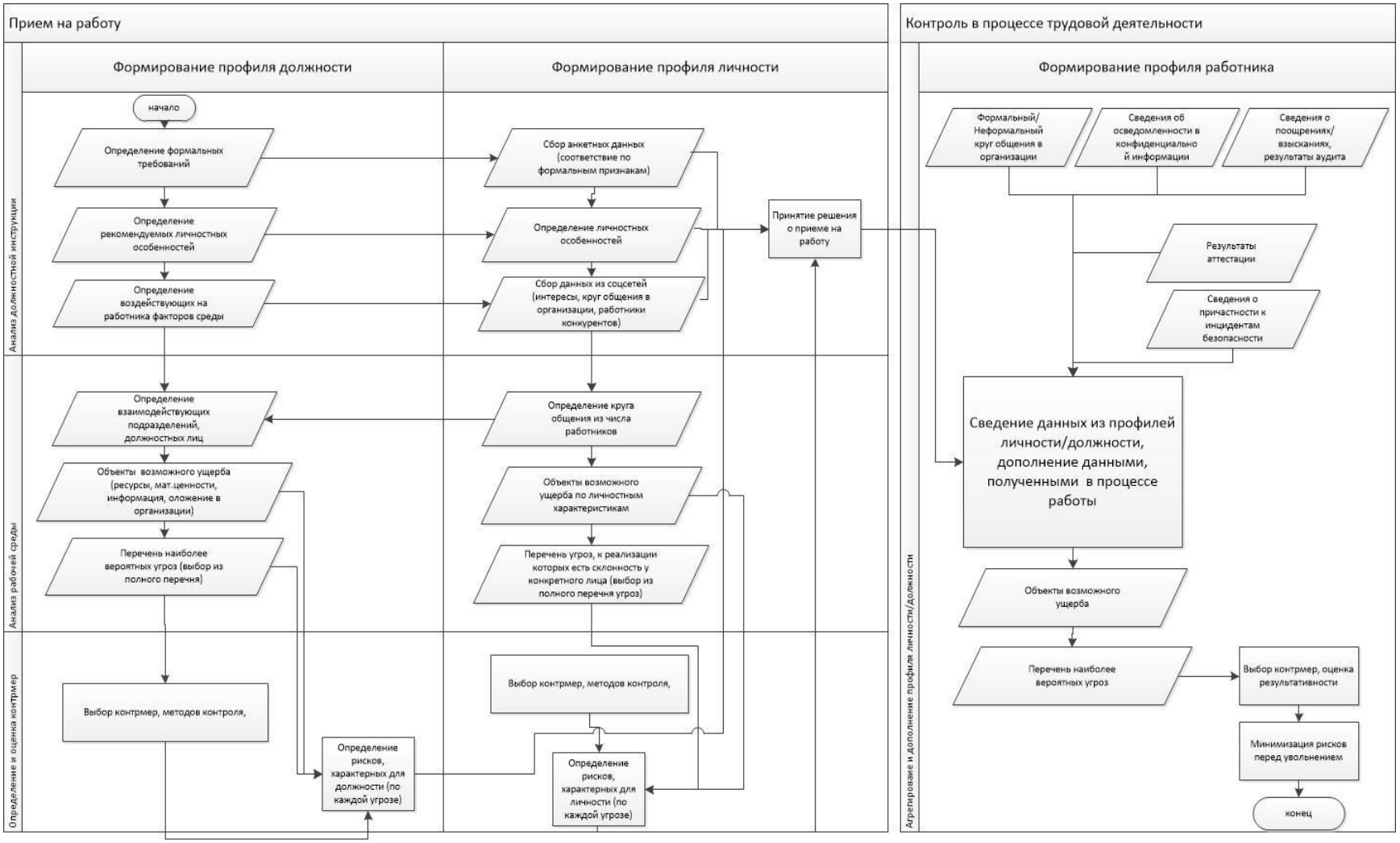
Заключение

Применение описанного в настоящей статье подхода в деятельности предприятия позволит уменьшить риски кадровой безопасности, увеличить степень автоматизации процесса оценки поступающих на работу, контроля за соблюдением уже работающих сотрудников, выработать комплекс организационных мероприятий, направленных на минимизацию ущерба компании при увольнении работника.

Список литературы

1. *Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017) "О персональных данных"* // СПС КонсультантПлюс.
2. *ГОСТ Р МЭК 61508-4-2012. Национальный стандарт Российской Федерации. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4.Термины и определения.* М.: Стандартинформ, 2008.
3. *ГОСТ Р 51898-2002. Аспекты безопасности. Правила включения в стандарты.* М.: ИПК Издательство стандартов, 2002.

4. *ГОСТ Р 52551-2006. Системы охраны и безопасности. Термины и определения.* М.: Стандартинформ, 2006.
5. Алавердов А.Р. *Управление кадровой безопасностью организации:* Учебник / Академическая серия М.: Изд. МАРКЕТ-ДС, 2008.
6. Кузнецова Н.В. Угрозы кадровой безопасности организации // *Известия ИГЭА.* 2014, № 2(94).
7. Стрыгина В.В. Профиль должности как системообразующий подход стандартизации должностей предприятия // *Социальная психология и общество* .2013, № 1.


Прием на работу
Контроль в процессе трудовой деятельности
Формирование профиля должности
Формирование профиля личности
Формирование профиля работника
Анализ должностной инструкции
Анализ рабочей среды
Определение и оценка контрмер
Агрегирование и дополнение профиля личности/должности
начало
Определение формальных требований
Определение рекомендуемых личностных особенностей
Определение воздействующих на работника факторов среды
Сбор анкетных данных (соответствие по формальным признакам)
Определение личностных особенностей
Сбор данных из соцсетей (интересы, круг общения в организации, работники конкурентов)
Принятие решения о приеме на работу
Определение взаимодействующих подразделений, должностных лиц
Объекты возможного ущерба (ресурсы, мат.ценности, информация, оложение в организации)
Перечень наиболее вероятных угроз (выбор из полного перечня)
Определение круга общения из числа работников
Объекты возможного ущерба по личностным характеристикам
Перечень угроз, к реализации которых есть склонность у конкретного лица (выбор из полного перечня угроз)
Выбор контрмер, методов контроля,
Определение рисков, характерных для должности (по каждой угрозе)
Выбор контрмер, методов контроля,
Определение рисков, характерных для личности (по каждой угрозе)
Формальный/ Неформальный круг общения в организации
Сведения об осведомленности в конфиденциально й информации
Сведения о поощрениях/ взысканиях, результаты аудита
Результаты аттестации
Сведения о причастности к инцидентам безопасности
Сведение данных из профилей личности/должности, дополнение данными, полученными в процессе работы
Объекты возможного ущерба
Перечень наиболее вероятных угроз
Выбор контрмер, оценка результативности
Минимизация рисков перед увольнением
конец