ПРОБЛЕМА АВТОМАТИЗАЦИИ МЕТОДИКИ ОЦЕНКИ КАНДИДАТОВ НА ВАКАНТНУЮ ДОЛЖНОСТЬ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О. О. Землянская, В. А. Ефремов
(Челябинск, ЮУрГУ (национальный исследовательский университет), olka-balolka@rambler.ru)

На сегодняшний день большинство организаций используют персональные компьютеры в своей деятельности, потому что это экономит человеческие ресурсы и время, позволяет получать точные результаты в короткий срок. Автоматизация процесса оказывает положительный эффект, но вместе с этим имеет факторы, которые могут вызывать затруднения в работе. Разработка и внедрение любой системы влечет за собой вопросы, на которые необходимо найти ответы, и множество задач, которые необходимо выполнить. Особенно остро это явление проявляется в разработке системы, не имеющей аналогов в открытых источниках. Таким образом, в данной работе затронуты проблемы автоматизации методики оценки кандидатов на вакантную должность в контексте информационной безопасности.

Все методы оценки «человеческого капитала» вырастают из единой потребности в измерении и контроле. Сложность создания таких методов заключается в сложности объекта измерения. Чтобы измерение стало возможным, человека нужно описать в виде набора объективных показателей и задать критерии для количественной оценки, которые возможны только для материальных предметов. Оценка, основанная на учете набора компетенций, позволяет сохранить положительные стороны интервью и в то же время добиться строгости и стандартизации [1]. Не менее актуальной является проблема объективности оценивания рекрутером, которая остается открытой и зависит от каждого оценщика индивидуально.

Созданная методика предназначена для использования при приеме сотрудника на работу, оценка кандидата совмещается с собеседованием, включает в себя тестирование на осведомленность в вопросах информационной безопасности, личные качества и поиск информации о кандидате в Интернете. В ходе собеседования со-

трудник отдела кадров заполняет ответы кандидата на вопросы анкеты, включающей в себя блоки по различным аспектам. Результатом является процентный показатель уязвимости: от 0 % (кандидат уязвим с точки зрения информационной безопасности) до 100 % (кандидат неуязвим) и графическое представление в виде диаграммы, разбитой по блокам [2].

Первым шагом автоматизации является разработка алгоритма. На данном этапе создан программный продукт UVIS v1.0, он является гибким, функциональным, учитывает специфику каждого структурного подразделения и степень конфиденциальности информации, с которой необходимо работать потенциальному сотруднику, и имеет дружественный интерфейс, обеспечивающий пользователю удобное взаимодействие с программой. Кроме того, существует разбиение программы на взаимосвязанные между собой модули, один из которых предназначен для оценщика («UVIS v1.0 Сотрудник»), другой – для оцениваемого («UVIS v1.0 Кандидат»). «UVIS v1.0 Сотрудник» представляет собой форму, которая заполняется сотрудником, содержит в себе такие поля, как «Фамилия Имя Отчество кандидата», «Структурное подразделение», «Категория», а также содержательную анкету и идентификатор, присвоенный данной форме. «UVIS v1.0 Кандидат» содержит в себе идентификатор и тест, на который отвечает кандидат самостоятельно.

Необходимо также учесть техническую часть: автоматизация невозможна без наличия оборудованного рабочего места, которое включает в себя персональный компьютер, принтер и доступ в Интернет. На настоящий момент практика показывает, что многие организации используют две операционные системы: Windows XP и Windows 7. Таким образом, разработчиком обеспечена работоспособность продукта на обеих операционных системах семейства Windows во всех существующих редакциях. В связи с тем, что доступ к персональному компьютеру необходим кандидату на вакантную должность, системному администратору нужно произвести настройки дополнительной учетной записи таким образом, чтобы не допустить несанкционированный доступ к файлам и папкам.

Большинство программ периодически обновляются. Разработчик дополняет свой продукт новыми функциями, изменяет внешний

вид, исправляет ошибки предыдущей версии. Этот аспект актуален для разработанной программы UVIS v1.0. Реализация обновления возможна путем скачивания новой версии программы, при этом перед разработчиком стоит задача обеспечения сохранности базы данных и специфичных настроек, присущих данной организации, в которой используется продукт.

Для того чтобы программа могла быть адаптирована в любой организации, она должна содержать в себе изменяемый блок вопросов, в котором отражена специфика сферы деятельности организации, отдельных структурных подразделений и должностей. Поставленная задача решена дополнительным модулем «UVIS v1.0. Конструктор», с помощью которого заказчик может сам составить вопросы, ответы на которые считает необходимыми для оценивания кандидата.

Важнейшим звеном в процессе оценки кандидата является сотрудник, который проводит оценку. На сегодняшний день большинство организаций оборудованы персональными компьютерами, ИТ-компетентный сотрудник такой компании легко освоит программный продукт. Проблему составляет процесс обучения персонала, чей уровень владения персональным компьютером низок. В таком случае есть несколько вариантов решения данного вопроса. Первый – отказаться от автоматизированной версии, провести оценку, имея анкету-опросник на бумажном носителе, второй – обучить сотрудника минимальному набору знаний, достаточных для осуществления оценки по внедряемой методике.

Таким образом, создан программный продукт на основе методики оценки кандидата на вакантную должность в контексте информационной безопасности. Со стороны пользователя данного продукта автоматизация процесса зависит от готовности как технической (наличие автоматизированного рабочего места и доступа в Интернет), так и кадровой (уровень владения персональным компьютером конечным пользователем). Нерешенными проблемами методики являются объективность оценщика и интерпретация нешаблонных ответов и фактов, касающихся оцениваемого. Открытым для разработчика остается вопрос процедуры обновления версии программы без потери базы данных и специфических настроек.

Библиографические ссылки

1. Измеряя неизмеримое : E-xecutive [Электронный ресурс]. Режим доступа : http://www.e-xecutive.ru/career/adviser/340036/.

2. *Астахова Л. В.*, *Землянская О. О.* Методика оценки кадровых уязвимостей информационной безопасности организации на этапе приема сотрудника на работу // Вестн. УрФО. Безопасность в информационной сфере. М., 2013. № 1(7). С. 53–58.

ПРАВОВЫЕ ВОПРОСЫ ВНЕДРЕНИЯ НОВОЙ СИСТЕМЫ ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ ФУНКЦИЙ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ

А. Н. Комиссаров[1], *Е. В. Рухлова*[2]
([1] Курган, КГУ, smack4ever@mail.ru;
[2] Челябинск, ЮУрГУ (национальный исследовательский университет), rukhlova-ekaterina@yandex.ru)

В юриспруденции под термином «тайна связи» понимается ценность, обеспечиваемая правом на тайну связи. На сегодняшний день право на тайну связи считается составной частью прав человека – (естественных прав личности). В Российской Федерации право на тайну связи (переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений) гарантируется Конституцией Российской Федерации (ч. 2, ст. 23). Эта же статья Конституции закрепляет положение о том, что ограничение права на тайну связи допускается только на основании судебного решения.

Однако в последнее время наметилась определенная тенденция по внесению изменений, направленных на ограничение права на тайну связи, в нормативно-правовые акты, призванные регулировать общественные отношения в области информационной безопасности. Так, благодаря выложенной в сеть Интернет информации компанией «ВымпелКом» интернет-пользователи узнали о готовящихся изменениях в Правила применения оборудования коммутации и маршрутизации пакетов информации сетей переда-