УДК 004.4.056 + 005.953.2.004.056
ББК У9(2)248

Астахова Л. В., Землянская О. О., Ефремов В. А.

АВТОМАТИЗАЦИЯ ОЦЕНКИ КАНДИДАТА НА ВАКАНТНУЮ ДОЛЖНОСТЬ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Вопросу анализа защищенности программно-технической составляющей информационных систем посвящено немало внимания, в то время как анализ защищённости пользователей информационных систем, т. е. кадровых уязвимостей информационной безопасности, находится на ранней стадии исследования. В статье охарактеризован созданный на основе авторской методики программный продукт «UVIS», позволяющий автоматизировать процесс оценки кандидата на вакантную должность в контексте информационной безопасности, описаны функциональные возможности его версий для оценщика и оцениваемого, а также проблемы его реализации. Особое внимание уделено уровню квалификации сотрудника, использующего программный продукт.

Ключевые слова: *оценка, уязвимость, кадровая безопасность, кандидат, информационная безопасность, автоматизация, программный продукт.*

Astakhova L. V., Zemlianskaya O. O., Efremov V. A.

AUTOMATIZATION OF THE ASSESSMENT OF A CANDIDATE FOR A VACANT POSITION OF ENSURING INFORMATION SECURITY IN THE ORGANIZATION

A great deal of attention is paid to the matter of protection of program and technical components of information systems while the analysis of protection of users of information systems (namely personnel vulnerability of information security) is on the earliest stage of its development. The article characterizes the software solution 'UVIS' based on unique method-

ology developed by the author. 'UVIS' allows automatization of the process of assessment of a candidate for a vacant position of ensuring information security in the organization, as well as the functional resources and opportunities of its versions for the assessor and the assesse, and problems of its implementation. Much attention is also paid to the level of qualification of the employee who uses the software.

Keywords: *assessment, vulnerability, personnel security, candidate, information security, automatization, software solution.*

Все методы оценки «человеческого капитала» возникают из потребности в его измерении и контроле. Сложность создания таких методов заключается в сложности объекта измерения. Чтобы измерение стало возможным, человека нужно охарактеризовать с помощью объективных количественных параметров, которые возможны только для материальных объектов. Однако попытки автоматизировать этот процесс предпринимаются в современной науке и практике. Так, специалисты СПИИРАН разрабатывают методы поиска вероятности успеха социоинженерного атакующего воздействия на пользователей информационной системы[1]. В их работах выявляются также взаимосвязи между психологическими особенностями, уязвимостями и возможными действиями пользователя информационной системы в рамках понятия социоинженерных атак[4]. Между тем, необходима методика перехода от исследований профиля психологических особенностей пользователя к профилю кадровых уязвимостей всех пользователей информационной системы в целом[2].

Созданная нами методика оценки кандидата[3] предназначена для использования при приеме сотрудника на работу. Оценка кандидата складывается из результатов собеседования, тестирования на осведомленность в вопросах информационной безопасности и поиска информации о кандидате в Интернете. Результатом являются процентный показатель уязвимости кандидата: от 0 % (кандидат уязвим с точки зрения информационной безопасности) до 100 % (кандидат неуязвим), а также графическое представление в виде диаграммы, разбитой по блокам. С целью автоматизации процесса оценки кандидата на вакантную должность нами создан программный продукт «UVIS v1.0».

Разработанный нами программный продукт 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. Программа имеет связанные между собой модули: «UVIS v1.0 Сотрудник» — предназначен для оценщика, «UVIS v1.0 Кандидат» — для оцениваемого. «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 анкету и идентификатор, присвоенный данной форме. «UVIS v1.0 Кандидат» содержит в себе идентификатор и тест, на который кандидат отвечает самостоятельно.

Автоматизация невозможна без наличия оборудованного рабочего места, которое включает в себя персональный компьютер, принтер и доступ в Интернет. Практика показывает, что многие организации используют две операционные системы: Windows XP и Windows 7. 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 необходимо произвести настройки дополнительной учетной записи таким образом, чтобы не допустить несанкционированного доступа к файлам и папкам.

Разработчик, как правило, дополняет свой продукт новыми функциями, изменяет внешний вид, исправляет ошибки предыдущей версии. Этот аспект актуален и 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. Он должен быть ИТ-компетентным, способным легко освоить программный продукт. Проблемой является 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, достаточному для осуществления оценки по внедряемой методике.

Таким образом, созданный программный продукт позволяет автоматизировать процесс 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.

Примечания

[1] Азаров, А. А. Ускорение расчетов оценки защищенности пользователей информационной системы за счет элиминации маловероятных траекторий социоинженерных атак / А. А. Азаров, А. Л. Тулупьев, Н. Б. Соловцов, Т. В. Тулупьева // Труды СПИИРАН. — 2013. — Вып. 2 (25). — С. 171—181.

[2] Астахова, Л. В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации / Л. В. Астахова // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление и радиоэлектроника». — 2013. — Т. 13. — № 1. — С. 79—83.

[3] Астахова, Л. В. Методика оценки кадровых уязвимостей информационной безопасности организации на этапе приема сотрудника на работу / Л. В. Астахова, О. О. Землянская // Вестник УрФО. Безопасность в информационной сфере. — 2013. — № 1. — С. 53—59.

[4] Ванюшичева, О. Ю. Количественные измерения поведенческих проявлений уязвимостей пользователя, ассоциированных с социоинженерными атаками / О. Ю. Ванюшичева, Т. В. Тулупьева, А. Е. Пащенко, А. Л. Тулупьев, А. А. Азаров // Труды СПИИРАН. — 2011. — Вып. 4 (19). — С. 34—47.

References

[1] Azarov, A. A., Tulup'ev, A. L., Solovtsov, N. B., Tulup'eva, T. V. Uskorenie raschetov otsenki zashchishchennosti pol'zovatelei informatsionnoi sistemy za schet eliminatsii maloveroyatnykh traektorii sotsio-inzhenernykh atak [Acceleration factor in estimation of protection of users of information systems due to elimination of low-probability trajectory of social and engineering attacks]//Trudy SPIIRAN.— 2013. — No. 2 (25).— P. 171—181.

[2] Astakhova, L. V. Problema identifikatsii i otsenki kadrovykh uyazvimostei informatsionnoi bezopasnosti organizatsii [Problem of identification and assessment of personnel vulnerability of information security]// Vestnik YuUrGU. Seriya Komp'yuternye tekhnologii, upravlenie i radioelektronika. — 2013. — Volume 13, No.1. — P. 79—83.

[3] Astakhova, L. V., Zemlyanskaya, O. O. Metodika otsenki kadrovykh uyazvimostei informatsionnoi bezopasnosti organizatsii na etape priema sotrudnika na rabotu [Methodology assessment of personnel vulnerability of information security on the stage of employee's employment]/ L. V. Astakhova, O. O. Zemlyanskaya // Vestnik UrFO. Bezopasnost' v informatsionnoi sfere. — 2013. — No.1.— P. 53—59.

[4] Vanyushicheva, O. Yu., Tulup'eva, T. V. , Pashchenko, A. E., Tulup'ev, A. L., Azarov, A. A. Kolichestvennye izmereniya povedencheskikh proyavlenii uyazvimostei pol'zovatelya, assotsiirovannykh s sotsioinzhenernymi atakami [Quantitative evaluation of behavioristic activity in user's vulnerability associated with sociological and engineer attacks]//Trudy SPIIRAN. — 2011. — No. 4 (19). — P. 34—47.

Астахова Людмила Викторовна, д. п. н., профессор, профессор кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: lvastachova@mail.ru

Землянская Ольга Олеговна, студент кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: olka-balolka@rambler.ru

Ефремов Виктор Александрович, студент кафедры «Безопасность информационных систем», Южно-Уральский государственный университет. E-mail: efremovva@bk.ru

Liudmila Viktorovna Astakhova, PhD Pedagogics, professor, professor of the Department of Information System Security of the South Ural State University. E-mail: lvastachova@mail.ru

Olga Olegovna Zemlianskaya, student of the Department of Information System Security of the South Ural State University. E-mail: olka-balolka@rambler.ru

Viktor Aleksandrovich Efremov, student of the Department of Information System Security of the South Ural State University. E-mail: efremovva@bk.ru