Published in the Slovak Republic
Vestnik policii
Has been issued since 2014.
ISSN: 2409-3610
E-ISSN: 2414-0880
2017, 4(1): 35-39

DOI: 10.13187/vesp.2017.1.35
www.ejournal21.com

UDC 004.056

The Concept of Suitability of Staff to Work with Confidential Information on the Basis of Personal Qualities

Natalya S. Ralnikova [a, *]

[a] ITMO University, Russian Federation

Abstract

Now in one of the existing international and domestic standards on information security as security vulnerabilities not mentioned personal qualities of staff and are not defined as methods of their evaluation. Meanwhile, the personal qualities included in the structure of professional competence of a specialist of any profile, and they constitute the essence of the concept "human factor", which is often the cause of loss and leakage of proprietary information.

This article raises the question of the impact of human factors on information security for the organization and the need for analytical work with staff before admission to confidential information, as well as when applying for a job. The author emphasizes that the importance of personal characteristics is not inferior to the importance of professional competence, if we are talking about information security.

In the article the author identifies the reasons for the negative impact on information security from staff, determines the most dangerous from the point of view of information security the personal characteristics of staff as the reasons for the negative impact on information security, and examines methods and tools for assessing personal qualities of personnel and carrying out analytical work.

Keywords: information security, staff, staffing the vulnerability assessment, the human factor.

1. Введение

Успешное функционирование любой организации зависит от уровня защищенности ее информационных ресурсов. Число утечек информации с каждым годом непрерывно растет, и по статистике в большинстве случаев виной тому собственный персонал организации (Астахова, 2015b; Ульянов, Астахова, 2014). Это говорит лишь о том, что человек как звено информационной системы серьезно недооценивается службами информационной безопасности.

Человеческий фактор играет важную роль в вопросах информационной безопасности. Персонал организации, обладающий конфиденциальной информацией и работающий с конфиденциальными документами, является наиболее трудно контролируемым и трудно управляемым источником угроз для информационной безопасности. Поэтому помимо

* Corresponding author
E-mail addresses: natalya.ralnikova@gmail.com (N.S. Ralnikova)

профессиональных качеств, каждый сотрудник, работающий с конфиденциальной информацией, должен обладать соответствующими моральными и личностными качествами (Родин, 2007).

Для снижения рисков информационной безопасности, связанной с персоналом, необходимо определить перечень личностных факторов, опасных с точки зрения информационной безопасности, а также методы их оценки. Перед допуском сотрудника к работе с конфиденциальными документами, он должен пройти соответствующую проверку.

2. Материалы и методы

Основными материалами для написания статьи послужили последние исследования специалистов в сфере угроз со стороны персонала на информационную безопасность организации и оценки кадровых уязвимостей.

Основными методами для исследования послужили общенаучные методы познания и анализа: в ходе написания статьи были проанализированы работы специалистов в данной сфере, а также комплексный подход к изучению проблемы.

3. Обсуждение

На данный момент в существующих стандартах по информационной безопасности в качестве уязвимостей информационной безопасности не названы личностные характеристики персонала и не определены методы их оценки. Между тем, человеческий фактор зависит не только от профессиональных компетенций сотрудников организации, т. е. способности конвертации их знаний, умений и навыков в практику, но и от личностно-ценностных компетенций (Ульянов, Астахова, 2014; Астахова, 2011) А ведь именно человеческий фактор зачастую является причиной утраты и утечки защищаемой информации.

Для определения требуемых личностных качеств специалиста, чья деятельность в организации связана с защитой информации, необходимо рассмотреть причины негативного воздействия на информационную безопасность со стороны персонала.

К преднамеренным причинам отнесем стремление нанести вред (отомстить) руководству или коллеге по работе; стремление обезопасить себя, родных и близких от угроз, шантажа, насилия; воздействие со стороны злоумышленника. К непреднамеренным – неквалифицированное выполнение операций; халатность, безответственность, недисциплинированность, недобросовестное отношение к выполняемой работе; небрежность, неосторожность, неаккуратность (Алексенцев, 2000).

Существует ограниченный набор личностных факторов, которые являются опасными с точки зрения утечки информации:

- болтливость;
- не умение хранить секреты;
- повышенная конфликтность;
- повышенная эмоциональность, вспыльчивость;
- недовольство своим положением;
- желание выделиться за счет других (карьеризм, эгоизм);
- любовь к вещам, к жизни на широкую ногу;
- повышенная внушаемость;
- подверженность манипуляциям;
- незаинтересованность в результатах труда;
- мстительность;
- склонность к риску;
- невнимательность (Журин, Калинкина, 2004; Астахова, Землянская, 2013).

Так, например, излишняя болтливость опасна с точки зрения информационной безопасности, так как сотрудник может раскрыть информацию ограниченного доступа посторонним людям. Мстительность может привести к стремлению сотрудника отомстить руководству или коллеге при конфликте или увольнении путем намеренного разглашения информации. Внимательность так же может послужить показателем в процессе оценки персонала, рассеянный сотрудник может потерять носители с конфиденциальной

информацией, а значит, представляет угрозу компании. Вспыльчивый сотрудник плохо контролирует себя в нестабильном состоянии, его легко выбить из колеи, чем может воспользоваться злоумышленник, и это приведет к разглашению конфиденциальной информации. Легко поддающийся к манипуляциям, соответственно, может быть подвержен манипуляции со стороны злоумышленника и разгласить конфиденциальную информацию, и так далее (Астахова, Землянская, 2013).

5. Результаты

В процессе допуска сотрудника к работе с конфиденциальными документами, необходимо проводить аналитическую работу по выявлению личностных качеств сотрудника для принятия решения о возможности его допуска.

Аналитическая работа может включать себя собеседование, где в процессе диалога при помощи специально подобранных вопросов выявляются личностные характеристики кандидата. Например, просьба рассказать о вчерашнем дне поможет выявить такое качество как болтливость, а вопрос «легко ли Вы прощаете людей?» – склонность к мести. Также, здесь можно использовать психологические тесты, например тест на внимательность, стресс-интервью или психологический тест «Подвержены ли вы манипуляции?» К. Бурениной (Буренина, 2014).

Помимо собеседования для сбора информации могут быть использованы такие методы как заполнение кандидатом специальной анкеты или наблюдение за работой сотрудника. Также можно использовать опрос с использованием полиграфа.

Также в ходе тестирования кандидата можно применить такой психологический прием как провокация на разглашение конфиденциальной информации.

Каждая из личностно-ценностных компетенций может быть отдельным показателем уязвимости информационной безопасности, каждому из которых руководством организации должны быть присвоены разные либо одинаковые коэффициенты значимости (Астахова, 2013)

В дополнение к оценке личностных качеств претендента следует использовать недавно появившийся способ – сбор и анализ информации о субъекте с помощью социальных сетей. Личная страничка в сети может многое поведать о жизни человека, его интересах и моральных принципах, а потому ее анализ страницы дополняет оценивание вышеуказанных блоков личностных качеств.

Факторами для оценки сотрудника могут являться:

- список интересуемых групп, страниц, на которые подписан пользователь;
- содержание анкеты, сообщений, фото- и видеоматериала;
- уровень конфиденциальности страницы, т.е. степени ограничения для разных категорий пользователей (это расскажет о наличии общих представлений о необходимости защиты конфиденциальной информации).

Также, запросы по фамилии, имени и отчеству в поисковых системах могут дать кое-какую информацию о человеке, с помощью чего можно сделать определенные выводы (Астахова, Землянская, 2013).

В результате данной аналитической работы мы получим некую картину психологических особенностей сотрудника. Для решения о допуске кандидата к конфиденциальной информации необходимо сравнить результаты проверки с документом, в котором описаны требования к качествам сотрудника для данной категории доступа. Этот документ может являться дополнением к должностной инструкции.

При категорировании сотрудников критериями могут быть ценность информации, с которой ему необходимо работать, а также частота обращения к конфиденциальной информации.

При наличии не критичного количества отрицательных факторов можно допустить сотрудника к работе с конфиденциальной информацией, несколько усилив организационно-технические меры безопасности для такого сотрудника. Обычно усиление мер защиты снижает вероятность совершения противоправных действий (Журин, Калинкина, 2004).

6. Заключение

Постоянный рост числа инцидентов информационной безопасности по вине персонала организации требует совершенствования методов службы безопасности работы с персоналом. Оценка личностно-ценностных компетенций сотрудников организации перед допуском к работе с конфиденциальными документами способна помочь в решении проблемы человеческого фактора в информационной безопасности объектов.

Кадровая безопасность является императивом деятельности по обеспечению информационной безопасности, а потому важнейшим объектом оценки. Целесообразна также разработка специального стандарта по критериям оценки доверия к кадровой безопасности информационной системы (Астахова, 2015).

Литература

Алексенцев, 2000 – *Алексенцев А.И.* Понятие и структура угроз защищаемой информации // Безопасность информационных технологий. М., 2000. № 3.

Астахова, 2011 – *Астахова Л.В.* Проблема оценки HR-уязвимости объекта защиты информации // Вестник УрФО. Безопасность в информационной сфере. М., 2011. № 1. С. 26-33.

Астахова, 2013 – *Астахова Л.В.* Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». М., 2013. № 1. С. 79-83.

Астахова, 2015a – *Астахова Л.В.* Доверие к кадровой безопасности информационной системы // Вестник УрФО. Безопасность в информационной сфере. М., 2015. 3. С. 33-36.

Астахова, 2015b – *Астахова Л.В.* Доверие к пользователю информационной системы как компонент доверия к ее безопасности // Наука ЮУрГУ: материалы 67-й научной конференции Секции технических наук. М., 2015. С. 682-687.

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

Буренина, 2014 – *Буренина К.* Офис. Стратегия выживания. Эксмо, 2014. 112 с.

Журин, Калинкина, 2004 – *Журин С.И., Калинкина М.Ю.* Вопросы оценки благонадежности персонала в подготовке администратора информационной безопасности // Защита информации. Конфидент, №3, 2004, с. 58-61.

Родин, 2007 – *Родин О.П.* Проблема персонала в сфере информационной безопасности // Вестник ТГУ. Том 4. Вып. 1. 2007, С. 164-165.

Ульянов, Астахова, 2014 – *Ульянов Н.Л., Астахова Л.В.* Проблема кадровой безопасности в системе стандартов информационной безопасности Банка России // Вестник УрФО. Безопасность в информационной сфере. М., 2014. № 4. С. 26-33.

References

Aleksentsev, 2000 – *Aleksentsev A.I.* (2000). Ponyatie i struktura ugroz zashchishchaemoi informatsii [The concept and structure of the protected information threats]. *Bezopasnost' informatsionnykh tekhnologiĭ*. № 3. [in Russian]

Astakhova, 2011 – Astakhova L.V. (2011). Problema otsenki HR-uyazvimosti ob"ekta zashchity informatsii [The problem of evaluation of HR-the vulnerability of the object of protection of the information]. *Vestnik UrFO*. Bezopasnost' v informatsionnoi sfere. № 1. S. 26-33. [in Russian]

Astakhova, 2013 – *Astakhova L.V.* (2013). Problema identifikatsii i otsenki kadrovykh uyazvimostei informatsionnoi bezopasnosti organizatsii [The problem of identification and evaluation of personnel security vulnerabilities of the organization]. *Vestnik YuUrGU. Seriya «Komp'yuternye tekhnologii, upravlenie, radioelektronika»*. № 1. S. 79-83. [in Russian]

Astakhova, 2015a – *Astakhova L.V.* (2015). Doverie k kadrovoi bezopasnosti informatsionnoi sistemy [The credibility of the HR information system security]. *Vestnik UrFO*. Bezopasnost' v informatsionnoi sfere. M., 3. S. 33-36. [in Russian]

Astakhova, 2015b – *Astakhova L.V.* (2015). Doverie k pol'zovatelyu informatsionnoi sistemy kak komponent doveriya k ee bezopasnosti [The credibility of the user of the information system as

a component of trust to it security]. Nauka YuUrGU: materialy 67-ĭ nauchnoi konferentsii Sektsii tekhnicheskikh nauk. M., S. 682-687. [in Russian]

Astakhova, Zemlyanskaya, 2013 – *Astakhova L.V., Zemlyanskaya O.O.* (2013). Metodika otsenki kadrovykh uyazvimostei informatsionnoi bezopasnosti organizatsii na etape priema sotrudnika na rabotu [Method of assessing personnel vulnerabilities of information security organization at the stage of admission of an employee]. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere*. M., № 1. S. 53-58. [in Russian]

Burenina, 2014 – *Burenina K.* (2014). Ofis. Strategiya vyzhivaniya [Office. Survival strategy]. Eksmo, 112 s. [in Russian]

Rodin, 2007 – *Rodin O.P.* (2007). Problema personala v sfere informatsionnoi bezopasnosti [The problem of personnel in the field of information security]. Vestnik TGU. Tom 4. Vyp. 1. S. 164-165. [in Russian]

Ul'yanov, Astakhova, 2014 – *Ul'yanov N.L., Astakhova L.V.* (2014). Problema kadrovoi bezopasnosti v sisteme standartov informatsionnoi bezopasnosti Banka Rossii [The problem of personnel security in the system of information security standards of the Bank of Russia]. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere*. M., № 4. S. 26-33. [in Russian]

Zhurin, Kalinkina, 2004 – *Zhurin S.I., Kalinkina M.Yu.* (2004). Voprosy otsenki blagonadezhnosti personala v podgotovke administratora informatsionnoi bezopasnosti. [The issues of assessing the trustworthiness of the staff in preparing information security administrator]. *Zashchita informatsii. Konfident*, №3, s. 58-61. [in Russian]

УДК 004.056

Принятие решения о пригодности персонала к работе с конфиденциальной информацией на основе личностных качеств

Наталья Сергеевна Ральникова [a, *]

[a] Университет ИТМО, Российская Федерация

Аннотация. В настоящее время ни в одном из существующих международных и отечественных стандартов по информационной безопасности в качестве уязвимостей информационной безопасности не названы личностные качества персонала и не определены методы их оценки. Между тем, личностные качества входят в структуру профессиональных компетенций специалиста любого профиля, и именно они составляют сущность понятия «человеческий фактор», являющийся, зачастую, причиной утраты и утечки защищаемой информации.

В данной статье поднимается вопрос влияния человеческого фактора на информационную безопасность организации и необходимости проведения аналитической работы с персоналом перед допуском его к конфиденциальной информации, а также при приеме на работу. Автором подчеркивается, что важность личностных характеристик, не уступает важности профессиональных компетенций, если речь идет об информационной безопасности.

В статье автор выделяет причины негативного воздействия на информационную безопасность со стороны персонала, определяет наиболее опасные с точки зрения информационной безопасности личностные характеристики персонала как причины негативного воздействия на информационную безопасность, а также рассматривает методы и средства для оценки личностных качеств сотрудников и проведения аналитической работы.

Ключевые слова: информационная безопасность, персонал, кадровая уязвимость, оценка, человеческий фактор.

* Корреспондирующий автор
Адреса электронной почты: natalya.ralnikova@gmail.com (Н.С. Ральникова)