

*Ю. С. Эстерле<sup>1</sup>*✉

## **Разработка методики оценки сформированности компетенций по информационной безопасности**

<sup>1</sup>Сибирский государственный университет геосистем и технологий,  
г. Новосибирск, Российская Федерация  
e-mail: j.khodoreva@gmail.com

**Аннотация.** Статья посвящена проблеме «человеческого фактора» как основной причины инцидентов информационной безопасности. Актуальность исследования обусловлена тем, что до 95 % утечек данных происходят по вине сотрудников, не обладающих достаточными компетенциями в области защиты информации. В работе представлена авторская методика оценки сформированности компетенций по информационной безопасности для неспециализированного персонала, включающая трёхуровневую матрицу компетенций. Матрица разработана по трем основным уровням сформированности компетенций: пороговый, базовый и повышенный. Также разработан диагностический инструментарий, включающий тест, анкету для оценки поведенческих привычек и кейс-метод. Разработанная методика позволяет не только констатировать уровень знаний сотрудников, но и выявлять конкретные слабые зоны для точечного обучения. Методика апробирована в условиях организации и может быть рекомендована к внедрению в системы корпоративного обучения.

**Ключевые слова:** информационная безопасность, человеческий фактор, компетенции, неспециализированный персонал, методика оценки, повышение осведомлённости

*I. S. Esterle<sup>1</sup>*✉

## **Development of a methodology for assessing the formation of information security competencies**

<sup>1</sup>Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation  
e-mail: j.khodoreva@gmail.com

**Abstract.** The article is devoted to the problem of the "human factor" as the main cause of information security incidents. The relevance of the study is due to the fact that up to 95 % of data leaks are caused by employees who do not have sufficient information security competencies. The paper presents an author's methodology for assessing the level of information security competencies for non-specialized personnel, which includes a three-level matrix of competencies. The matrix is divided into three main levels of competency development: threshold, basic, and advanced. A diagnostic toolkit has also been developed, which includes a test, a questionnaire for assessing behavioral habits, and a case study method. The developed methodology allows not only to assess the level of employees' knowledge, but also to identify specific weaknesses for targeted training. The methodology has been tested in an organization and can be recommended for implementation in corporate training systems.

**Keywords:** information security, human factor, competencies, non-specialized personnel, assessment methodology, awareness raising

## ***Введение***

Современное общество и экономика всё в большей степени зависят от цифровых технологий и информационных систем. На фоне активной цифровизации государственных, корпоративных и образовательных процессов вопросы информационной безопасности приобретают особую значимость. При этом источником инцидентов в этой сфере нередко становятся не внешние атаки, а действия или бездействие самих сотрудников, не обладающих необходимыми знаниями и навыками в области защиты информации.

Согласно данным аналитических центров 70 %-90 % инцидентов связаны с действиями людей, не соответствующими установленным нормативным требованиям. В основном это ошибки конфигурации, разглашение данных, фишинг, использование слабых паролей, а также несоблюдение регламентов безопасности [1, 2]. Особенно остро стоит проблема недостаточной сформированности компетенций по информационной безопасности у неспециализированного персонала – это сотрудники, чья профессиональная деятельность не связана напрямую с обеспечением защиты информации, но они ежедневно работают с информационными системами, электронными документами или корпоративной почтой.

Несмотря на осознание данной проблемы, в настоящее время отсутствует универсальный и систематизированный подход к оценке уровня сформированности компетенций по информационной безопасности у неспециализированного персонала. Существующие методики либо ориентированы на специалистов в данной области, либо имеют узконаправленный, формальный характер, не позволяющий получить объективную и комплексную оценку реальных знаний и навыков пользователей [3].

Цель исследования: разработка методики оценки сформированности компетенций по информационной безопасности для неспециализированного персонала.

Для достижения поставленной цели в работе поставлены и решены следующие задачи:

1. проведён анализ существующих подходов к оценке компетенций в области ИБ;
2. выявлены ключевые угрозы, связанные с человеческим фактором;
3. разработана трёхуровневая матрица компетенций для неспециализированного персонала;
4. создан диагностический инструментарий;
5. определена процедура проведения оценки;
6. проведена апробация методики в условиях организации табл. 1.

Теоретические основы исследования: Термин «человеческий фактор» впервые введён в научно-технической сфере для описания несоответствий, возникающих в результате невнимательности, халатности и недостаточной осведомлённости сотрудников [4]. Исследования единогласно указывают на то, что человеческий фактор является главной причиной нарушения безопасности информации. По данным

аналитических отчётов за 2024 – 2025 годы, около 5 % утечек информации связаны с действиями внутренних нарушителей [1; 2]. Приводится пример утечки, вызванной человеческим фактором, произошедшей в феврале 2024 года, где в открытом доступе около двух лет находились данные австрийской футбольной федерации. Для общего доступа были выставлены паспортные данные сотрудников, персональная информация о болельщиках и сведения о контрактах игроков. Дело в том, что разработчик случайно оставил ссылку на сервер в коде, доступном для просмотра.

Действия персонала, приводящие к реализации угроз, обусловлены комплексом факторов, которые разделяют на индивидуальные и организационные. Индивидуальные факторы включают в себя психофизиологические состояния, будь то усталость или стресс; личностные особенности, такие как невнимательность; профессиональные качества, а именно некомпетентность. К организационным факторам относятся неблагоприятные условия труда, недостаточная мотивация, неясность формулировок требований и отсутствие культуры безопасности [5]. В основе разработанной методики лежит компетентности подход, активно используемый в управлении персоналом с восьмидесятых годов XX века. Родоначальником подхода можно считать Дэвида Макклеланда [6]. Компетенции консолидируют способности и мотивацию, описывая производственное поведение сотрудника. Оценка персонала с помощью компетентностного подхода заключается в сопоставлении проявляемых поведенческих характеристик работника с эталонным набором.

Методика включает три основных компонента: авторскую матрицу компетенций, сформированный диагностический инструментарий и порядок процедуры проведения оценки.

Матрица компетенций. Для неспециализированного персонала выделены 7 ключевых компетенций (К1–К7), охватывающих все аспекты базовой грамотности в сфере информационной безопасности:

1. К1 – оценка роли информации и информационной безопасности в современном обществе;
2. К2 – оценка последствий нарушения конфиденциальности, целостности и доступности информации;
3. К3 – оценка рисков управления доступом;
4. К4 – безопасные практики работы в сетях;
5. К5 – защита персональных данных;
6. К6 – противодействие социальной инженерии и фишингу;
7. К7 – безопасность устройств и программного обеспечения.

На основе сформированных и сформулированных компетенций разработан диагностический инструментарий, а также проведена апробация разработанной методики табл. 1, табл. 2.

## ***Методы и материалы***

**Таблица 1.** Состав участников апробации методики

| № | Должность                | Стаж работы в организации | Пол |
|---|--------------------------|---------------------------|-----|
| 1 | Менеджер по продажам     | 2 года                    | М   |
| 2 | Бухгалтер                | 5 лет                     | Ж   |
| 3 | Сотрудник отдела кадров  | 1 год                     | Ж   |
| 4 | Специалист отдела кадров | 3 года                    | Ж   |
| 5 | Экономист                | 4 года                    | Ж   |
| 6 | Администратор офиса      | 6 месяцев                 | Ж   |

**Таблица 2.** Индивидуальные результаты сотрудников

| Должность                | Стаж   | Баллы | %     | Уровень     |
|--------------------------|--------|-------|-------|-------------|
| Менеджер по продажам     | 2 года | 24    | 80 %  | Продвинутый |
| Бухгалтер                | 5 лет  | 27    | 90 %  | Продвинутый |
| Сотрудник отдела кадров  | 1 год  | 21    | 70 %  | Базовый     |
| Специалист отдела кадров | 3 года | 27    | 90 %  | Продвинутый |
| Экономист                | 4 года | 30    | 100 % | Продвинутый |
| Администратор офиса      | 6 мес. | 18    | 60 %  | Базовый     |

## ***Обсуждение***

Полученные результаты подтверждают, что разработанная методика позволяет дифференцировать сотрудников по уровню сформированности компетенций даже на благополучной выборке, где нет сотрудников с низким уровнем знаний. Средний процент правильных ответов в тесте (81,8 %), средний процент безопасности в анкете (84,7 %) и средний процент выполнения кейсов (81,7 %) свидетельствуют о том, что сотрудники, участвующие в апробации, в целом обладают достаточным уровнем грамотности.

## ***Заключение***

В ходе проведённого исследования разработана и апробирована методика оценки сформированности компетенций по информационной безопасности для неспециализированного персонала. Основные выводы: трёхуровневая матрица компетенций позволяет дифференцировать сотрудников по категориям; комплексный диагностический инструментарий даёт объективную оценку знаний, поведенческих привычек и практических навыков; апробация на выборке из 6 сотрудников подтвердила работоспособность методики.

Разработанная методика является практически применимым инструментом для объективной оценки уровня знаний таких сотрудников и может быть рекомендована к внедрению в системы корпоративного обучения.

#### БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Отчет о глобальных рисках за 2022 год // Всемирный экономический форум. URL: [https://www3.weforum.org/docs/WEF\\_The\\_Global\\_Risks\\_Report\\_2022.pdf](https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf).
2. Positive Technologies. Киберугрозы: основные тенденции 2022 года. URL: <https://www.ptsecurity.com/research/analytics/cybersecurity-threatscape-2022/>
3. Кибанов А.Я., Митрофанова Е.А., Коновалова В.Г., Чуланова О.Л. Концепция компетентностного подхода в управлении персоналом: монография. М.: НИЦ ИНФРА-М, 2014. 156 с.
4. Самарская Н.А. Влияние человеческого фактора на трансформацию охраны труда в контексте современной теории поколений // Лидерство и менеджмент. 2023. Т. 10. № 3. С. 837–856.
5. Searchinform. 48% российских компаний сталкивались с утечками информации по вине сотрудников. 2025. URL: <https://searchinform.ru/news/company-news/2025/2/20/48-of-russian-companies-have-experienced-information-leaks-caused-by-employees/>.

© Ю. С. Эстерле, 2026