УДК 004.056.5, 629.5.067

doi: 10.53816/23061456_2024_11–12_9

# ОЦЕНКА КАЧЕСТВА РАБОТЫ СОТРУДНИКА ДЕПАРТАМЕНТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

# ASSESSMENT OF THE QUALITY OF WORK OF AN EMPLOYEE OF THE INFORMATION TECHNOLOGY DEPARTMENT OF AN INDUSTRIAL ENTERPRISE IN ENSURING INFORMATION SECURITY

*С.И. Фокина, А.В. Выволокина*

*S.I. Fokina, A.V. Vyvolokina*

*Санкт-Петербургский государственный морской технический университет*

В статье предложен набор показателей, применимый для моделирования и оценки качества работы сотрудников отделов информационных технологий судостроительных предприятий, а также для оценки качества процесса организации администрирования и работы. Обозначены основные параметры качества работы сотрудника информационной безопасности предприятия. Выявлена необходимость поиска решений, способных дать количественную оценку важным качествам специалиста информационных технологий (ИТ). Приведены формульные зависимости для расчета стохастических показателей, позволяющих получить объективные оценки субъективного влияния человеческого фактора на безопасное функционирование информационных систем промышленных предприятий. Модель может быть использована для поддержки принятия решений по совершенствованию системы и организации и планирования противодействию угрозам информационной безопасности (ИБ).
***Ключевые слова:*** показатели качества, информационная безопасность, информационная система, ИТ-специалист, противодействие угрозам.

The article proposes a set of indicators applicable for modeling and assessing the work quality of employees in information technology departments of shipbuilding enterprises, as well as for evaluating the quality of administration and work organization processes. Key parameters of the quality of work of an information security employee at an enterprise are identified. The need for finding solutions capable of quantitatively assessing the critical qualities of an information technology specialist is highlighted. Formulaic dependencies are provided for calculating stochastic indicators, which allow for objective evaluations of the subjective influence of the human factor on the secure functioning of industrial enterprises' information systems. The model can be used to support decision-making aimed at improving system organization and planning measures to counteract information security threats.
***Keywords:*** quality indicators, information security, information system, IT-specialist, countering threats.

## Вводная часть

Процессы информатизации, связанные с управлением жизненным циклом изделий и проектов, демонстрируют экспоненциальный рост. Значительно увеличиваются показатели компьютерной преступности в организации промышленного шпионажа, мошенничестве в банковско-финансовой сфере и в области нарушения конституционных прав и свобод человека и гражданина. Происходит взлом частной информации (несанкционированное проникновение), растут масштабы и количество скоординированных компьютерных атак на финансово-экономические и военно-стратегические объекты.

Работа по защите объектов в целях противодействия угрозам информационной безопасности требует от соответствующих специалистов непрерывного исследования больших объемов данных, что подразумевает набор компетенций, необходимых для этого. Многие современные сотрудники ИТ-служб проводят рабочее и внерабочее время, совершенствуя защиту и управление большими данными. Организация значительного количества цифровых данных, полученных при выполнении некоторых работ, таких как протоколы собраний, обучающие видео, фотографии, отчеты и инструкции, также может оказывать влияние на качество работы ИТ-специалиста.

Несмотря на внедрение систем поддержки принятия решений на основе искусственного интеллекта в целях повышения оперативности и обоснованности реагирования на угрозы, решающее слово остается за человеком.

В ходе анализа когнитивных задач специалистов по информационной безопасности установлено, что при решении своих функциональных задач этим специалистам приходится осуществлять мониторинг данных, переходя от общих сигналов и предупреждений к конкретным деталям инцидентов, чтобы принимать решения о том, что следует рассматривать как опасность, а что нет, и какие действия могут иметь различный уровень опасности в каждой конкретной ситуации [1]. Уровень подготовки специалиста по безопасному управлению информационной инфраструктурой оценивается по тому, как быстро он обнаружил вторжения, оповестил уполномоченных коллег о вторжении, а также выбрал и осуществил необходимые меры противодействия [2].

## Основная часть

Предположим, что функционирование любого объекта можно представить набором параметров, значения которых могут изменяться в заданных диапазонах своих значений (то есть информационной «надежности»). Каждый из таких параметров рассматривается с позиций сопротивляемости возможным отказам под действием внешних воздействий, которые в свою очередь определяют ограничения на изменения значений анализируемых параметров. В этом случае, сочетая параметры воздействий и сопротивляемости, на основе физических законов природы можно построить модель безопасного функционирования информационных систем (ИС) с учетом изменения во времени предельных значений рассматриваемых параметров, которая в отличие от математических моделей теории надежности становится пригодной для прогнозирования безопасной работы ИС в зависимости от качеств специалиста. В такой модели сам перечень этих параметров будет характеризовать функциональность объекта.

Анализ подходов к оценке качества подготовки специалиста ИТ [3, 4] показал, что спектр показателей достаточно широк, поэтому обычно рассматриваются только наиболее важные из них, определенные профессиональным стандартом: оперативность, устойчивость, непрерывность и скрытность (добавим к ним современное требование — качество защиты).

Как видно в таблице, ряд показателей носит случайный характер и в качестве их оценки используются вероятности. Приведем некоторые решения, способные дать количественную оценку важным качествам специалиста ИТ [5, 6].

1. Вероятность своевременного обеспечения работы ИС предприятия для информации *i*-го приоритета в заданное время $T_{Zi}$ можно рассчитать, если представить систему связи как систему массового обслуживания, в которой заявками на обслуживание будут запросы от абонентов на устранение угроз ИБ:

$$P_{si}\left(T_{Zi}\right) = \int_0^{\theta_i} \exp\left(-\tau\right)\tau^{\gamma_i} d\tau \,/\, \Gamma\left(\gamma_i\right),$$

*Таблица*

***Основные параметры качества работы сотрудника информационной безопасности предприятия***

| Требования к сотруднику ИБ | Параметры системы ИС, влияющие на выполнение функционала | Оцениваемые показатели качества |
|---|---|---|
| Качество | – обеспечение качественной защиты ИС сотрудником ИТ | – вероятность своевременного обеспечения работы ИС предприятия |
| Оперативность | – среднее время на купирование угрозы ИТ;<br>– оперативность информационного обмена (документальной информацией) | – время устранения инцидента;<br>– пропускная способность сотрудника ИТ |
| Непрерывность | – количество отказов системы за единицу времени;<br>– среднее время восстановления работоспособности | – коэффициент готовности сотрудника ИТ;<br>– среднее время восстановления системы |
| Скрытность | – обеспечение передачи информации требуемого уровня конфиденциальности;<br>– сокрытие от злоумышленника структуры ИС | – высший приоритет купируемой угрозы;<br>– вероятность сохранения защищенности информации в течение периода ее объективной актуальности |
| Устойчивость | – среднее время восстановления ИС при повреждении от внешних воздействий;<br>– надежность системы | – нормативное время на восстановление повреждений;<br>– нормативное время передачи управления на не атакованный узел управления ИС;<br>– вероятность обеспечения работоспособного состояния в заданное время |

где $\Gamma(\gamma)=\int_0^{\theta_i}\exp(-\tau)\tau^{\gamma_i}d\tau$ — табулируемая неполная гамма-функция;

$$\gamma_i=\frac{T_{pi}}{\sqrt{T_i-T_{pi}^2}};\quad \theta_i=T_{Zi}\cdot\frac{\gamma_i^2}{T_{pi}},$$

где $\gamma_i$, $\theta_i$ — рассчитываемые параметры неполной гамма-функции;

$T_{pi}$ и $T_i$ — рассчитываемые соответственно среднее время и момент времени реакции специалиста ИБ при обработке запросов *i*-го типа в системе (полного времени пребывания на обработке с учетом ожидания в очереди).

Исходными данными для оценки показателей являются: $I$ — общее количество возможных приоритетов запросов на предотвращение угроз и $\lambda_i$ — интенсивность потока запросов *i*-го приоритета ($i=\overline{1,I}$).

2. Вероятность сохранения информации в течение периода ее объективной актуальности можно рассчитать, используя формулу:

$$P_c=1-\prod_{m=1}^{k}P_{pr\_m},$$

где $k$ — количество уровней защиты информации, которые требуется преодолеть злоумышленнику для доступа к ней, либо к ресурсам ИС;

$P_{pr\_m}$ — вероятность преодоления злоумышленником *m*-го уровня защиты информации. При этом для экспоненциальной аппроксимации распределений исходных характеристик при их независимости $P_{pr\_m}$ вычисляется по формуле:

$$P_{pr\_m}=\frac{f_m}{f_m+u_m},$$

где $f_m$ — среднее время между проверками параметров защиты *m*-го уровня;

$u_m$ — среднее время, затрачиваемое на преодоление *m*-го уровня защиты.

3. Вероятность обеспечения работоспособного состояния формально можно представить как

$$P_{rs}=F(t_i<T).$$

В значительной мере конкретное значение $t_i$ зависит от подготовленности оператора — сотрудника ИТ. Для случая максимума

неопределенности [7, 8], когда время восстановления работоспособности носит равномерный характер на интервале от минимального до предельного, формула выглядит так:

$$P_{rs} = \frac{(t_{\max} - t_{\min}) \times \text{random}}{T}.$$

Остальные предложенные показатели качества функционирования ИС являются ее техническими и эксплуатационными характеристиками и могут быть получены из их технической документации или из нормативных документов по организации информационного взаимодействия на предприятии.

Помимо технических характеристик при оценке сотрудника необходимо учитывать и финансовые затраты на его обучение и содержание. Здесь представляется целесообразным использовать два показателя качества: показатель стоимости задействованных средств и показатель затрат на услуги [9].

## Заключение

Предложенная модель позволяет учесть факторы, влияющие на качество сотрудника информационной безопасности предприятия, и на этой основе рассчитывать коэффициент вероятности, характеризующий качество всей информационной системы. Исходными данными для модели являются статистические данные о предыдущем этапе эксплуатации и опыте сотрудника [10].

Модель также может быть использована для поддержки принятия решений по совершенствованию системы, организации и планирования противодействию угрозам информационной безопасности и возможностям информационной системы в целом.

## Список источников

1. Авдеев М.М., Анисимов В.Г., Анисимов Е.Г. и др. Информационно-статистические методы в управлении микроэкономическими системами. Санкт-Петербург, Тула: Международная академия информатизации, 2001. 139 с.

2. Анисимов В.Г., Анисимов Е.Г., Мартыщенко Л.А., Шатохин Д.В. Методы оперативного статистического анализа результатов выборочного контроля качества промышленной продукции. Санкт-Петербург, Тула: Международная академия информатизации. 2001. 72 с.

3. Анисимов В.Г., Ведерников Ю.В., Гарькушев А.Ю., Сазыкин А.М. Научно-методическое сопровождение интеграции высокотехнологичных инноваций в процессы разработки высокоточного оружия // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2014. № 3–4. С. 66–75.

4. Анисимов В.Г., Гарькушев А.Ю., Сазыкин А.М. Оптимизация внедрения новых технологий в перспективные образцы артиллерийского вооружения // Известия Российской академии ракетных и артиллерийских наук. 2012. № 4 (74). С. 39–44.

5. Гарькушев А.Ю., Сазыкин А.М. и др. Основы построения моделей интеллектуализации в системах безопасности // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2014. № 9–10. С. 22–27.

6. Пряхин Е.И., Ларионова Е.В., Сазыкин А.М., Гарькушев А.Ю. Защита продукции оборонного назначения от контрафакта // Известия Российской академии ракетных и артиллерийских наук. 2014. № 1 (81). С. 113–118.

7. Сильников М.В., Ямпольский С.М., Шаламов А.С. и др. Концептуальные основы информационно-аналитического обеспечения органов управления военной организацией государства // Известия Российской академии ракетных и артиллерийских наук. 2016. № 4 (94). С. 9–15.

8. Карпова И.Л., Курилов А.В., Супрун А.Ф., Иванова Л.А. Учет влияния человеческого фактора в моделях кибербезопасности // Проблемы информационной безопасности. Компьютерные системы. 2023. № 2 (54). С. 27–36.

9. Ведерников Ю.В., Гарькушев А.Ю., Карпова И.Л., Супрун А.Ф. Формализация задачи выбора варианта структурного построения информационного комплекса управления многоуровневой иерархической системой по критерию информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 78–82.

10. Гарькушев А.Ю., Липис А.В., Супрун А.Ф., Иванова Л.А. Формирование культуры цифровой безопасности студентов высших учебных заведений судостроительного профиля // Про-

блемы информационной безопасности. Компьютерные системы. 2023. № 1 (53). С. 54–61.

**References**

1. Avdeev M.M., Anisimov V.G., Anisimov E.G. et al. Informacionno-statisticheskie metody` v upravlenii mikroe`konomicheskimi sistemami [Information and statistical methods in the management of microeconomic systems] / Mezhdunarodnaya akademiya informatizacii. Sankt-Petersburg, Tula. 2001. 139 p.

2. Anisimov V.G., Anisimov E.G., Marty`shhenko L.A., Shatoxin D.V. Metody` operativnogo statisticheskogo analiza rezul`tatov vy`borochnogo kontrolya kachestva promy`shlennoj produkcii / Mezhdunarodnaya akademiya informatizacii. Sankt Peterburg, Tula. 2001. 72 p.

3. Anisimov V.G., Vedernikov Yu.V., Gar`kushev A.Yu., Sazy`kin A.M. Nauchno metodicheskoe soprovozhdenie integracii vy`sokotexnologichny`x innovacij v processy` razrabotki vy`sokotochnogo oruzhiya // Voprosy` oboronnoj texniki. Seriya 16. Texnicheskie sredstva protivodejstviya terrorizmu. 2014. № 3–4. Pp. 66–75.

4. Anisimov V.G., Gar`kushev A.Yu., Sazy`kin A.M. Optimizaciya vnedreniya novy`x texnologij v perspektivny`e obrazcy artillerijskogo vooruzheniya // Izvestiya Rossijskoj akademii raketny`x i artillerijskix nauk. 2012. № 4 (74). Pp. 39–44.

5. Gar`kushev A.Yu., Sazy`kin A.M. i dr. Osnovy` postroeniya modelej intellektualizacii v sistemax bezopasnosti // Voprosy` oboronnoj texniki. Seriya 16. Texnicheskie sredstva protivodejstviya terrorizmu. 2014. № 9–10. Pp. 22–27.

6. Pryaxin E.I., Larionova E.V., Sazy`kin A.M., Gar`kushev A.Yu. Zashhita produkcii oboronnogo naznacheniya ot kontrafakta // Izvestiya Rossijskoj akademii raketny`x i artillerijskix nauk. 2014. № 1 (81). Pp. 113–118.

7. Sil`nikov M.V., Yampol`skij S.M., Shalamov A.S. et al. Konceptual`ny`e osnovy` informacionno-analiticheskogo obespecheniya organov upravleniya voennoj organizaciej gosudarstva // Izvestiya Rossijskoj akademii raketny`x i artillerijskix nauk. 2016. № 4 (94). Pp. 9–15.

8. Karpova I.L., Kurilov A.V., Suprun A.F., Ivanova L.A. Uchyot vliyaniya chelovecheskogo faktora v modelyax kiberbezopasnosti // Problemy` informacionnoj bezopasnosti. Komp`yuterny`e sistemy`. 2023. № 2 (54). Pp. 27–36.

9. Vedernikov Yu.V., Gar`kushev A.Yu., Karpova I.L., Suprun A.F. Formalizaciya zadachi vy`bora varianta strukturnogo postroeniya informacionnogo kompleksa upravleniya mnogourovnevoj ierarxicheskoj sistemoj po kriteriyu informacionnoj bezopasnosti // Problemy` informacionnoj bezopasnosti. Komp`yuterny`e sistemy`. 2018. № 3. Pp. 78–82.

10. Gar`kushev A.Yu., Lipis A.V., Suprun A.F., Ivanova L.A. Formirovanie kul`tury` cifrovoj bezopasnosti studentov vy`sshix uchebny`x zavedenij sudostroitel`nogo profilya // Problemy` informacionnoj bezopasnosti. Komp`yuterny`e sistemy`. 2023. № 1 (53). Pp. 54–61.