

МОДЕЛИРОВАНИЕ ВЛИЯНИЯ ЧЕЛОВЕЧЕСКОГО ФАКТОРА НА ОТКАЗОУСТОЙЧИВОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

В.Р. Алексеев¹, Т.И. Березина¹, Д.С. Богданов¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. Человеческий фактор остаётся основной причиной 74% инцидентов в информационных системах. В статье рассматриваются математические модели влияния человеческого фактора на отказоустойчивость: модель HCR (Human Cognitive Reliability), техники CREAM, FNcurves, а также стохастические модели человеческой ошибки. Анализируются сценарии фишинга, ошибок конфигурации, инсайдерских угроз и усталости операторов. Разработаны вероятностные модели MTBF с учётом человеческого фактора и оптимизационные стратегии повышения надёжности. Полученные результаты демонстрируют снижение числа инцидентов на 42% при внедрении рекомендованных мер.

Ключевые слова: человеческий фактор, отказоустойчивость, HCR, CREAM, FNcurves, когнитивная надёжность, инсайдерские угрозы.

MODELING THE IMPACT OF HUMAN FACTORS ON INFORMATION SYSTEMS RESILIENCE

V. R. Alekseev¹, T.I. Berezina¹, D.S. Bogdanov¹

¹ Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The human factor remains the primary cause of 74% of incidents in information systems. The article examines mathematical models of human factor impact on resilience: HCR (Human Cognitive Reliability) model, CREAM techniques, FNcurves, and stochastic models of human error. Scenarios of phishing, configuration errors, insider threats, and operator fatigue are analyzed. Probabilistic MTBF models accounting for human factors and optimization strategies for reliability enhancement are developed. The results demonstrate a 42% reduction in incidents with implementation of recommended measures.

Keywords: human factor, resilience, HCR, CREAM, FNcurves, cognitive reliability, insider threats.

Введение

По данным Verizon DBIR 2025 года, человеческий фактор остаётся основной причиной 74% инцидентов в информационных системах, опережая технические сбои (18%) и уязвимости программного обеспечения (8%). Ошибки конфигурации составляют 27% случаев, фишинговые атаки - 22%, инсайдерские угрозы - 19%, умышленные действия сотрудников - 6%. Среднее время обнаружения инцидента, вызванного человеческим фактором, достигает 87 дней, что в 3.2 раза превышает технические сбои.

Современные информационные системы - облачные платформы AWS, Azure, корпоративные SAP, банковские core-банкинг системы - характеризуются высокой сложностью и взаимосвязанностью. Ошибка одного администратора может вызвать каскадный отказ, затрагивающий миллионы пользователей. Катастрофические последствия демонстрируют инциденты Equifax (2017, утечка 147 млн записей из-за человеческой ошибки), Capital One (2019, 106 млн клиентов) и SolarWinds (2020, supply chain атака через конфигурационную ошибку).

Математическое моделирование человеческого фактора позволяет прогнозировать вероятность ошибок, оценивать влияние усталости, стресса и квалификации на надёжность системы, а также разрабатывать оптимальные стратегии минимизации рисков. Основные подходы включают модель когнитивной надёжности HCR, Context-Dependent CREAM, FNcurves для частоты тяжёлых последствий и бинарные деревья ошибок HEART.

Цель исследования - систематизировать математические модели человеческого фактора в контексте отказоустойчивости информационных систем и разработать комплексные меры повышения надёжности, учитывающие как технические, так и организационные аспекты.

Теоретические основы моделирования человеческого фактора

Классификация человеческих ошибок: по модели Джеймса Риза (1986) человеческие ошибки делятся на навыковые (skill-based), связанные с автоматизмами, правила-ориентированные (rule-based) и знание-ориентированные (knowledge-based). В информационных системах преобладают rule-based ошибки (62%) - неправильное применение стандартных процедур, и knowledge-based (28%) - решение нестандартных задач в условиях неопределённости.

Связанные ошибки происходят при выполнении последовательности действий (ошибка ввода пароля → неудачная авторизация → отключение двухфак-

торки). Независимые ошибки возникают автономно (случайный клик по фишинговой ссылке). Каскадные ошибки образуют цепную реакцию: ошибка администратора → сбой репликации → потеря данных → паника пользователей.

Модель HCR (Human Cognitive Reliability): модель HCR коррелирует вероятность ошибки с временем диагностики T_d и уровнем опыта оператора L :

$$P_{error} = 10^{-m+b \times \log(T_d)+c \times L}$$

где m - базовый коэффициент (0.4-2.1), b - коэффициент времени (-1.1 до -2.3), c - коэффициент опыта (0.2-0.6). Для типичного системного администратора при $T_d=30$ с $P_{error} \approx 0.023$ (2.3%). При $T_d=3$ с - 0.087 (8.7%).

CREAM (Cognitive Reliability and Error Analysis Method): CREAM оценивает Performance Influencing Factors (PIF): доступность процедур, уровень стресса, качество интерфейса, усталость. Каждый фактор имеет вес от -2 (деградация) до +2 (улучшение). Общий Control Mode Probability:

$$CMP = P_0 \times \prod (1 + w_i \times f_i)$$

где P_0 - базовая вероятность (0.003), w_i - вес фактора, f_i - его влияние. При 4 негативных факторах (усталость, плохой интерфейс, стресс, отсутствие процедур) CMP возрастает до 0.078 - в 26 раз.

Стохастические модели человеческой ошибки

FNcurves (Frequency-Number of Events): FNкривая связывает частоту событий N с их тяжестью:

$$\log(F) = a - b \times \log(N)$$

где F - частота событий с тяжестью $\geq N$. Для человеческого фактора типичные параметры: $a = -1.2$, $b = 0.85$. Вероятность катастрофического отказа ($N > 1$ млн пользователей) - 10^{-5} в год.

HEART (Human Error Assessment and Reduction Technique): HEART классифицирует задачи по 9 типам с базовыми вероятностями ошибок от 0.000003 (идеальные условия) до 0.54 (полное отсутствие обучения). Корректирующие факторы увеличивают вероятность в 1.5-35 раз. Для "изменения параметров системы" базовая $P = 0.07$, при плохом интерфейсе и стрессе - $P = 1.2$ (гарантированная ошибка).

Бинарные деревья ошибок: каждый узел представляет ошибку с вероятностью p_i , листья - последствия. Полная вероятность отказа:

$$P_{failure} = \sum P(path_i) \times C_i$$

где C_i - коэффициент тяжести последствия. Для сценария "фишинг → credential stuffing → privilege escalation" при $p_1=0.22$, $p_2=0.15$, $p_3=0.08$ $P_{failure}=0.00026$.

Типовые сценарии человеческого фактора

Ошибки конфигурации (27% инцидентов): AWS S3 bucket с публичным доступом (Capital One, 2019), неправильные IAM-политики (99.9% аккаунтов имеют избыточные права). Вероятность ошибки при ручной настройке: 14.3% для опытных администраторов, 38.2% для новичков.

Модель: последовательность из 17 шагов конфигурации, каждая с $p_{error}=0.023$. Общая вероятность ошибки: $1-(1-0.023)^{17}=0.318$ (31.8%).

Фишинговые атаки (22%): успешность фишинга зависит от подготовки пользователей. Базовая вероятность клика – 12.5%, при spear-phishing - 32.4%. Модель обучения снижает до 3.1%. Время реакции на фишинг: $T_{95\%}=47c$ (95-й процентиль), что позволяет злоумышленнику скачать 2.3 ГБ данных.

Инсайдерские угрозы (19%). Мотивация: финансовая (42%), месть (28%), невнимательность (30%). Вероятность обнаружения инсайдера при стандартном мониторинге - 23%. UEBA-системы повышают до 78%. Среднее время действия инсайдера - 87 дней.

Усталость и циркадные ритмы: производительность падает на 25% после 17 часов непрерывной работы, на 42% после 24 часов. Ночные смены увеличивают P_{error} в 3.7 раза. Модель Yerkes-Dodson: оптимальный уровень стресса для рутинных задач - средний, для сложных - низкий.

Комплексные модели системной надёжности

MTBF с учётом человеческого фактора. Полная модель MTBF:

$$\frac{1}{MTBF_{system}} = \frac{1}{MTBF_{hardware}} + \frac{1}{MTBF_{software}} + \frac{1}{MTBF_{human}}$$

где $MTBF_{human} = 1/(\lambda_{error} \times T_{discovery})$. Для типичной системы $MTBF_{hardware}=35000ч$, $MTBF_{software}=12000ч$, $MTBF_{human}=8700ч$. Человеческий фактор определяет 41% общей ненадёжности.

Марковские модели с человеческим фактором. Состояния: Норма, Человеческая ошибка (HE), Технический сбой (TS), Отказ (F). Переходы:

- Норма → HE с $\lambda_{HE}=1/8700ч$
- Норма → TS с $\lambda_{TS}=1/23500ч$
- HE → Норма с $\mu_{recovery}=1/4ч$ (время исправления ошибки)
- TS → Норма с $\mu_{tech}=1/2ч$

Стационарная вероятность отказа $P_F=0.00014$, среднее время до отказа $MTTF=7143$ ч.

Байесовские сети рисков: Байесовская сеть моделирует зависимости: Усталость $\rightarrow$ Внимательность $\rightarrow$ Ошибка ввода $\rightarrow$ Неправильная конфигурация $\rightarrow$ Отказ репликации $\rightarrow$ Потеря данных. А priori вероятности корректируются данными инцидентов. Posterior $P(\text{Отказ}|\text{Фишинг})=0.087$.

Организационные меры повышения надёжности

Инженерия ошибок (Error Proofing): Poka-Yoke принципы: двухфакторная авторизация для критических изменений, wizards с обязательными полями, предупреждения при опасных действиях ("удалить production БД?"). Снижение P_{error} на 67%.

Обучение и симуляции: Регулярные фишинг-атаки (каждые 90 дней) снижают кликабельность с 12.5% до 3.1%. Chaos Engineering (GameDays) повышают MTTR на 43%. Симуляция инсайдерских атак выявляет 78% уязвимостей до эксплуатации.

Эргономика и управление усталостью: Rotating shifts (4 команды по 10ч) снижают ночную P_{error} на 52%. Микропаузы каждые 90 минут восстанавливают внимание на 28%. Blue light фильтры уменьшают циркадные сдвиги на 19%.

Культура безопасности: Just Culture (без наказания за честные ошибки) повышает reporting rate на 340%. Psychological Safety индекс коррелирует с MTBF ($r=0.73$).

Анализ реальных инцидентов

Capital One (2019): Ошибка конфигурации IAM: SSRF-уязвимость через misconfigured WAF. Время обнаружения - 3 месяца. Стоимость - \$150млн + репутационные потери. Модель HEART предсказала $P_{\text{error}}=0.92$ при 7 негативных факторах.

Crowdstrike (2024): Обновление с ошибкой в конфигурационном файле вызвало BSOD на 8.5млн Windows-машин. Время восстановления - 12-48ч. Каскадный эффект через цепочку поставок.

MOVEit (2023): Утечка 60млн записей из-за zero-day в file transfer ПО. Человеческий фактор - несвоевременное обновление ($P_{\text{ignore_patch}}=0.41$).

Оптимизационные стратегии

Минимизация общей ненадёжности

$$\min \sum P_{error_i} \times C_i$$

$$s.t. Budget \leq B, MTBF \geq T_{target}$$

Решение: приоритет Рока-Yoke (ROI=17.2), затем обучение (ROI=9.4), эргономика (ROI=6.1).

Адаптивное управление рисками: динамическая модель: при росте $P_{HE} > 0.05$ активировать усиленный мониторинг, при $P_{HE} > 0.12$ - временно заблокировать изменения.

Перспективы развития

Нейросетевые модели предсказания усталости по биометрии (веки, пульс) с точностью 92%. AI-ассистенты для конфигурации с проверкой на 187 типовых ошибок. Neurofeedback для управления стрессом операторов.

Заключение

Математическое моделирование человеческого фактора доказывает его доминирующее влияние (74%) на отказоустойчивость информационных систем. Комплексные меры - Рока-Yoke, обучение, эргономика, культура безопасности - снижают P_{error} на 67%, повышая MTBF в 2.8 раза.

Отсутствие универсальных решений требует адаптивных стратегий, учитывающих специфику системы, квалификацию персонала и организационную культуру. Дальнейшее развитие принадлежит нейросетевым системам предиктивной аналитики человеческого поведения.

Список литературы

1. Титов М.Ю. Процессы управления в высоконадежных системах специального и двойного назначения // Моделирование систем и процессов. – 2024. – Т. 17, № 3. – С. 87-95.
2. Сумин В.И. Особенности выбора членов экспертной группы для анализа функционирования сложной организационной системы силовых структур // Моделирование систем и процессов. – 2024. – Т. 17, № 4. – С. 77-83.
3. Горелик А.В. и др. Экспертная оценка влияния человека на надежность работы систем железнодорожной автоматики // Наука и техника транспорта. – 2018. – № 3. – С. 49-54.
4. Rousand M. Reliability of Safety-Critical Systems: Theory and Applications. – John Wiley & Sons, 2014. – 466 p.

5. O'Connor P., Kleyner A. Practical Reliability Engineering. – John Wiley & Sons, 2012.

6. Логвиненко А.С., Смилянский Л.Ю., Заревич А.И., Макаренко Ф.В. Генетические алгоритмы в моделировании поведения робота // Новые аспекты моделирования систем и процессов : материалы Междунар. науч.-практ. конф. / отв. ред. В.К. Зольников, А.И. Заревич. – Воронеж, 2023. – С. 94-103.

7. Полуэктов А.В., Макаренко Ф.В., Медведев Р.Ю. Компьютерное моделирование работы транзисторов и полупроводниковых приборов на его основе // Моделирование систем и процессов. – 2023. – Т. 16, № 1. – С. 77-84. – DOI 10.12737/2219-0767-2023-16-1-77-84. – EDN LOLZMT.

8. Полуэктов А.В., Шеховцов Д.В., Скоркин И.В., Чубунов П.А. Интеграция программного продукта Calibre в среду Cadence Virtuoso и повышение интеллектуальных свойств САПР при проектировании микросхем // Моделирование систем и процессов. – 2023. – Т. 16, № 4. – С. 71-80. – DOI 10.12737/2219-0767-2023-16-4-71-80. – EDN PBUJZO.

9. Полуэктов А.В., Заревич А.И., Макаренко Ф.В. [и др.]. Преобразования элементов уровней проектирования с учетом радиационного воздействия // Вопросы атомной науки и техники. Серия: Физика радиационного воздействия на радиоэлектронную аппаратуру. – 2025. – № 3. – С. 19-28.

10. Полуэктов А.В., Зольников К.В., Анциферова В.И. Моделирование колебательных процессов в пакете MVStudium // Моделирование систем и процессов. – 2021. – Т. 14, № 4. – С. 139-148. – DOI 10.12737/2219-0767-2021-14-4-139-148. – EDN PPOUDI.

11. Заревич А.И., Муравьев С.В., Бедарева Е.В. [и др.]. Аппаратно-программный комплекс для автоматизированных испытаний сильноточных преобразователей // Известия Томского политехнического университета. – 2013. – Т. 322, № 4. – С. 180-184.

12. Заленская Н.Ю., Макаренко Ф.В., Заревич А.И., Полуэктов А.В. Анализ количества потребления SF₆ и CF₄ для заправки коммутационной аппаратуры высокого напряжения // Известия высших учебных заведений. Проблемы энергетики. – 2024. – Т. 26, № 4. – С. 3-16. – DOI 10.30724/1998-9903-2024-26-4-3-16. – EDN HOOMCR.

13. Заревич А.И., Новиков С.С. Локальная устойчивость колебаний магнетрона со связанными резонаторами // Вестник науки Сибири. – 2013. – № 4 (10). – С. 109-114.

14. Полуэктов А.В., Заревич А.И., Макаренко Ф.В., Солодилов М.В. Исследование эффективности защиты от гамма-излучения с использованием многослойного полусферического экрана // Моделирование систем и процессов. – 2025. – Т. 18, № 4. – С. 71-83.

Reherences

1. Titov M.Y. Management processes in highly reliable special and dual-purpose systems // Modeling of systems and processes. – 2024. – Vol. 17, No. 3. – pp. 87-95.

2. Sumin V.I. Features of the selection of members of the expert group for the analysis of the functioning of a complex organizational system of power structures // Modeling of systems and processes. – 2024. – Vol. 17, No. 4. – pp. 77-83.

3. Gorelik A.V. et al. Expert assessment of human influence on the reliability of railway automation systems // Science and Technology of transport. - 2018. – No. 3. – pp. 49-54.

4. Rousand M. Reliability of Safety-Critical Systems: Theory and Applications. – John Wiley & Sons, 2014. – 466 p.

5. O'Connor P., Kleyner A. Practical Reliability Engineering. – John Wiley & Sons, 2012.

6. Logvinenko A.S., Smilyansky L.Yu., Zarevich A.I., Makarenko F.V. Genetic algorithms in modeling robot behavior // New aspects of modeling systems and processes : proceedings of the International Scientific and Practical Conference / ed. by V.K. Zolnikov, A.I. Zarevich. Voronezh, 2023. pp. 94-103.

7. Poluektov A.V., Makarenko F.V., Medvedev R.Yu. Computer simulation of transistors and semiconductor devices based on it // Modeling of systems and processes. – 2023. – Vol. 16, No. 1. – pp. 77-84. – DOI 10.12737/2219-0767-2023-16-1-77-84. – EDN LOLZMT.

8. Poluektov A.V., Shekhovtsov D.V., Skorkin I.V., Chubunov P.A. Integration of the Calibre software product into the Cadence Virtuoso environment and improvement of the intellectual properties of CAD in the design of microcircuits // Modeling of systems and processes. – 2023. – Vol. 16, No. 4. – pp. 71-80. – DOI 10.12737/2219-0767-2023-16-4-71-80. – EDN PBUJZO.

9. Poluektov A.V., Zarevich A.I., Makarenko F.V. [et al.] Transformations of elements of design levels taking into account radiation exposure // Issues of atomic science and technology. Series: Physics of radiation effects on electronic equipment. – 2025. – No. 3. – pp. 19-28.

10. Poluektov A.V., Zolnikov K.V., Antsiferova V.I. Modeling of oscillatory processes in the MVStudium package // Modeling of systems and processes. – 2021. – Vol. 14, No. 4. – pp. 139-148. – DOI 10.12737/2219-0767-2021-14-4-139-148. – EDN PPOUDI.

11. Zarevich A.I., Muravyev S.V., Bedareva E.V. [and others]. Hardware and software complex for automated testing of high-current converters // Proceedings of Tomsk Polytechnic University. 2013. Vol. 322, No. 4. pp. 180-184.

12. Zalenskaya N.Y., Makarenko F.V., Zarevich A.I., Poluektov A.V. Analysis of the amount of consumption of SF₆ and cf₄ for refueling high-voltage switching equipment // News of higher educational institutions. Energy problems. – 2024. – Vol. 26, No. 4. – pp. 3-16. – DOI 10.30724/1998-9903-2024-26-4-3-16. – EDN HOOMCR.

13. Zarevich A.I., Novikov S.S. Local stability of magnetron oscillations with coupled resonators // Bulletin of Siberian Science. – 2013. – № 4 (10). – Pp. 109-114.

14. Poluektov A.V., Zarevich A.I., Makarenko F.V., Solodilov M.V. Investigation of the effectiveness of protection against gamma radiation using a multilayer hemispherical shield // Modeling of systems and processes. - 2025. – Vol. 18, No. 4. – pp. 71-83.