ОЦЕНКА УЯЗВИМОСТЕЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ С ПРИМЕНЕНИЕМ ТЕОРИИ ВЕРОЯТНОСТЕЙ, РАСПРЕДЕЛЕНИЯ СТЬЮДЕНТА И НОРМАЛЬНЫХ СЛУЧАЙНЫХ ВЕЛИЧИН

Атласов И. В.[1], Ефимов А. О.[2], Рогозин Е. А.[3], Черкасова А. С.[4]

DOI: 10.21681/2311-3456-2025-2-124-131

Цель исследования: *изучение показателей и математических методов оценки уязвимостей автоматизированных систем. Рассмотрение применимости теории вероятностей, распределения Стьюдента и нормальных случайных величин в целях комплексной оценки уязвимостей.*

Метод(ы) исследования: *теория вероятностей, распределения Стьюдента и нормальных случайных величин. В качестве объекта исследования выступает автоматизированная система, имеющая количественные показатели (по количеству компонентов и количеству уязвимостей в них).*

Результат(ы) исследования: *полученные математические модели оценки уязвимостей значительно снижают уровень неопределенности, связанный с определением критичности угроз и их вероятности. Использование статистических методов, таких как теория вероятностей и распределение Стьюдента, позволяет создать более объективную и воспроизводимую оценку уязвимостей, исключая из процесса субъективные факторы. В частности, применение таких методов помогает учесть различные вариации в параметрах уязвимостей, таких как вероятность их эксплуатации, возможные последствия и риски, что делает процесс более точным и ориентированным на реальные данные. Это особенно важно в ситуациях, когда необходимо работать с ограниченными или неполными данными, как, например, при оценке новых или малозаметных уязвимостей.*

Кроме того, эти модели способствуют значительному снижению влияния человеческого фактора, что критично для обеспечения объективности и стабильности оценки. Если в традиционных методах анализа важным элементом является экспертная оценка, то математические модели позволяют свести к минимуму необходимость в субъективных решениях, что, в свою очередь, повышает точность и снижает вероятность ошибок, обусловленных личной интерпретацией данных. В итоге использование таких моделей приводит к более автоматизированному и объективному процессу оценки уязвимостей, что способствует улучшению управления рисками в области информационной безопасности и повышению защищенности автоматизированных систем.

Научная новизна: *заключается в применении теории вероятностей, распределения Стьюдента и нормальных случайных величин в целях снижения неопределенности при оценке уязвимостей автоматизированных систем, предложенные модели, в отличие от существующих, позволяют применять численные показатели, полученные экспериментальным путем, в отличие от методик (например, CVSS), использующих экспертную оценку.*

Вклад соавторов: *Рогозин Е. А. – общее руководство и верификация полученных результатов; Ефимов А. О. – анализ предметной области, постановка и формализация задачи применения теории вероятностей, распределения Стьюдента и нормальных случайных величин в целях оценки уязвимостей программного обеспечения; Атласов И. В. и Черкасова А. С. – реализация и описание математического аппарата, описание примера оценки.*

Ключевые слова: *математическое моделирование, статистические методы, снижение неопределенности, количественные показатели, информационная безопасность, анализ рисков, автоматизированные системы.*

1 Атласов Игорь Викторович, доктор физико-математических наук, профессор. Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В. Я. Кикотя», Москва. E-mail: atlasov.igor.777@gmail.com

2 Ефимов Алексей Олегович. Федеральное государственное казенное образовательное учреждение высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации», Воронеж. E-mail: ea.aleksei@yandex.ru

3 Рогозин Евгений Алексеевич, доктор технических наук, профессор. Федеральное государственное казенное образовательное учреждение высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации», Воронеж. E-mail: evgenirogozin@yandex.ru

4 Черкасова Анастасия Сергеевна. Федеральное государственное казенное образовательное учреждение высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации», Воронеж. E-mail: cherkasova.30@yandex.ru

Введение

Проблема оценки защищенности автоматизированных систем (АС) с учетом уязвимостей является комплексной задачей. Ее решение должно основываться на разработке решения, учитывающего все актуальные факторы, влияющие на уровень защищенности АС. Принцип системного подхода к исследованию вопросов защищенности предполагает[5] [1–11]:

1. Проведение анализа всех возможных угроз безопасности информации в АС.
2. Изучение параметров качества и эффективности функционирования базового комплекта средств защиты информации (СЗИ).
3. Выбор базового комплекта СЗИ на основе оптимальных параметров их эффективности, обеспечивающих необходимый уровень защищенности с минимальным влиянием на производительность АС.
4. Обеспечение защиты на всех этапах жизненного цикла АС, включая защиту каждой составной части системы.
5. Оценку критичности уязвимостей, выявленных в АС.
6. Анализ безопасности обновлений компонентов АС в защищенном исполнении.

Для детального изучения отдельных аспектов теории оценки защищенности АС проведен общий анализ указанных проблем.

Определение 1. Под уязвимостью АС понимается недостаток или слабость программного, программно-технического средства или информационной системы в целом, что может быть использовано для реализации угроз безопасности информации.

Основные цели информационной безопасности (ИБ) определяются задачами, выполняемыми базовым комплектом средств защиты информации (СЗИ) в автоматизированных системах (АС), выполненных в защищенном исполнении. Устранение уязвимостей является одной из ключевых задач ИБ, и цели ее достижения можно сформулировать следующим образом [11–20]:

- ❖ обеспечение защиты от использования уязвимостей для хищения информации (конфиденциальность);
- ❖ предотвращение использования уязвимостей для изменения или подмены информации (целостность);
- ❖ защита от использования уязвимостей, нарушающих работу технических средств обработки и передачи информации (доступность).

Определение 2. Под критичностью уязвимости понимается совокупность технических характеристик уязвимости программного обеспечения, аппаратного обеспечения и встроенного ПО. Эта совокупность выражается числовой оценкой, которая показывает серьезность уязвимости в сравнении с другими.

Системный подход к исследованию уязвимостей основан на трех ключевых принципах: целостности, сложности и цели.

Принцип целостности предполагает рассмотрение уязвимости АС как единого целого с собственной динамикой развития и спецификой.

Принцип сложности отражает объективные трудности в исследовании уязвимостей и их обнаружении, требует разработки количественных и качественных критериев для оценки критичности уязвимостей.

Принцип цели ориентирован на анализ того, каким образом уязвимость может быть использована и каковы последствия ее эксплуатации.

Системный подход предполагает необходимость проведения более глубокого анализа, охватывающего все аспекты оценки критичности уязвимости в сочетании с применяемыми средствами защиты и системами.

Уязвимости АС могут быть эффективно оценены с использованием теории вероятностей, распределения Стьюдента и нормальных случайных величин, что позволяет учитывать неопределенность и делать анализ объективным и воспроизводимым.

Теория вероятностей дает возможность оценивать вероятность успешной эксплуатации уязвимостей и общего риска, связанного с ними, а нормальные случайные величины позволяют моделировать параметры уязвимостей, такие как время обнаружения или сложность эксплуатации, и выявлять критичные отклонения.

Распределение Стьюдента применяется для анализа малых выборок данных, характерных для новых или редких уязвимостей, что позволяет проводить точное сравнение их параметров.

Такой подход снижает влияние человеческого фактора, заменяя субъективные экспертные оценки на количественные показатели, полученные экспериментально, и позволяет не только оценивать текущие уязвимости, но и прогнозировать их появление, что упрощает управление рисками и оптимизирует ресурсы на устранение наиболее критичных уязвимостей. В результате создается комплексная система анализа, способная повысить уровень защищенности АС даже в условиях ограниченности данных.

5 ГОСТ Р 58142-2018. Информационная безопасность. Методы и средства защиты информации. Общие положения. – Введ. 2018-12-01. – М.: Стандартинформ, 2018. – 24 с.
ГОСТ Р 56546-2015. Информационная безопасность. Защита информации. Показатели защищённости информационных систем. – Введ. 2016-01-01. – М.: Стандартинформ, 2016. – 12 с.
ГОСТ Р 53114-2008. Информационная технология. Защита информации. Основные термины и определения. – Введ. 2009-01-01. – М.: Стандартинформ, 2009. – 14 с

Проведём анализ существующих решений и публикаций по предметной области. В стандарте[6] [9] установлены основные положения и показатели защищенности информационных систем, регламентирующие подходы к защите информации и определяющие базовые термины, и параметры оценки.

В стандарте[7] [10] вводится терминологическая база для унификации подходов к защите информации. В работе [2] предложена оценка защищенности компьютерных сетей с использованием метрик CVSS, что позволяет количественно измерять уровень уязвимостей и проводить сравнительный анализ угроз. Схожие задачи представлены в [5], где разработан метод комбинированного анализа параметров для выявления уязвимостей на основе данных систем мониторинга.

Исследование [3] анализирует взаимосвязь между компонентами безопасности и надежностью защиты информации, предлагая обоснование показателей надежности. Работа [20] развивает эти подходы, рассматривая методики оценки надежности систем защиты от несанкционированного доступа. В публикации [4] представлены модели контроля доступа для защиты от атак на уязвимости приложений, а методика, предложенная в [16], включает классификацию уязвимостей для их формализации в рамках информационных систем.

Документ OWASP[8] [7] предлагает методику оценки рисков, фокусируясь на ранжировании угроз, что схоже с методикой оценки критичности уязвимостей, утвержденной ФСТЭК России[9].

Исследование [12] изучает технологии статического и динамического анализа уязвимостей, в то время как работы зарубежных исследователей [15], а также [13] демонстрируют эффективность применения глубокого обучения для автоматизированного выявления уязвимостей в программном коде.

В исследованиях [17] рассматривается системно-кибернетический подход к интеллектуальной защите информации, что коррелирует с работой, изучающей оценку безопасности облачных ИТ-компонент.

Работа [8] систематизирует источники данных об уязвимостях, что согласуется с задачами Taint-Scope, китайскими исследователями [14], направленными на автоматическое выявление программных уязвимостей с использованием алгоритмов тестирования некорректными данными.

Концептуальные основы оценки уязвимостей автоматизированных систем представлены в работе [11], где описаны методические подходы к анализу угроз и разработке программно-методических комплексов для повышения защищенности систем. В спецификациях CVSS v4.0[10] [6] предложены обновленные критерии оценки уязвимостей, что позволяет учитывать их критичность и влияние на информационные системы в условиях современных угроз.

Построение нормальных случайных величин

Выберем натуральные числа n, m, l, такие что справедливо равенство $n = ml$. Здесь считаем $n = 1000$ и $l = 50$.

Далее рассмотрим n испытаний АС, для каждого испытания устраиваем атаку на систему и проверяем как реагирует исследуемый элемент на работу системы.

В результате система может как обнаружить нападение, так не обнаружить его. Для каждого i: $1 \le i \le n$ испытания построим случайную величину ξ_i, принимающую два значения 1 и 0 в зависимости от того, отреагировала система на атаку или нет.

$$\xi_i = \begin{cases} 1, \text{ система отреагировала на атаку} \\ \quad \text{с вероятностью } p = P(\xi_i = 1) \\ 0, \text{ система не отреагировала на атаку} \\ \quad \text{с вероятностью } q = P(\xi_i = 0) \end{cases}, \quad (1)$$

где $p + q = 1$ и значения этих величин неизвестны. Предположим, что случайные величины $\{\xi_i\}_{i=1}^{n}$ независимы в совокупности, то есть справедливо равенство

$$P(\xi_1 < t_1, \dots, \xi_n < t_n) = P(\xi_1 < t_1) \dots P(\xi_n < t_n), \quad (2)$$

справедливое для всех действительных чисел $\{t_i\}_{i=1}^{n}$. Это условие говорит о том, что атаки на систему производятся независимо друг от друга.

Нам понадобится еще одно определение.

Определение 3. Пусть задана последовательность функций $\{f_n(x)\}_{n=1}^{\infty}$ и функция $f(x)$ со значениями в множестве действительных чисел, заданных для всех $x \in D$, где D – замыкание некоторого открытого множества на прямой.

Скажем, что последовательность функций $\{f_n(x)\}_{n=1}^{\infty}$ равномерно сходится к функции $f(x)$, если для некоторого $\varepsilon > 0$ существует натуральное n_0, такое что для всех натуральных $n > n_0$ справедливо равенство

$$|f_n(x) - f(x)| < \varepsilon \quad (3)$$

для всех $x \in D$. Обозначим этот факт через $f_n(x) \longrightarrow f(x)$.

Заметим, что случайная величина ξ_i обладает математическим ожиданием $M(\xi_i) = 1 \cdot p + 0 \cdot q = p$.

6 ГОСТ Р 56546-2015. Информационная безопасность. Защита информации. Показатели защищённости информационных систем. – Введ. 2016-01-01. – М.: Стандартинформ, 2016. – 12 с.

7 ГОСТ Р 53114-2008. Информационная технология. Защита информации. Основные термины и определения. – Введ. 2009-01-01. – М.: Стандартинформ, 2009. – 14 с.

8 OWASP Foundation. OWASP Risk Rating Methodology [Электронный ресурс]. – URL: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

9 Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств: утв. ФСТЭК России 28 октября 2022 г.: методический документ ФСТЭК России от 28.02.2022 г. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2

10 Forum of Incident Response and Security Teams. Common Vulnerability Scoring System version 4.0: Specification Document [Электронный ресурс]. – URL: https://www.first.org/cvss/specification-document

Квадрат случайной величины ξ_i^2 также обладает математическим ожиданием $M(\xi_i^2) = 1^2 \cdot p + 0^2 \cdot q = p$. Поэтому случайная величина ξ_i обладает дисперсией

$$D(\xi_i) = M(\xi_i^2) - M^2(\xi_i) = p - p^2 = pq. \quad (4)$$

Согласно центральной предельной теореме для одинаково распределенных случайных величин, имеющих дисперсию [1], справедливо утверждение,

$$P\Big(\frac{1}{\sqrt{lD(\xi_i)}} \sum_{k=1}^{l} \big(\xi_{l\cdot(j-1)+k} - M(\xi_i)\big) < t\Big) =$$

$$= P\Big(\frac{1}{\sqrt{lpq}} \sum_{k=1}^{l} \big(\xi_{l\cdot(j-1)+k} - p\big) < t\Big) \longrightarrow \frac{1}{2\pi} \int_{-\infty}^{t} e^{-\frac{x^2}{2}}\, dx, \quad (5)$$

которое означает, что для некоторого $\varepsilon > 0$ существует натуральное n_0, такое что для всех натуральных $l > n_0$ справедливо равенство:

$$\Big|P\Big(\frac{1}{\sqrt{lpq}} \sum_{k=1}^{l} \big(\xi_{l\cdot(j-1)+k} - p\big) < t\Big) - \frac{1}{2\pi} \int_{-\infty}^{t} e^{-\frac{x^2}{2}}\, dx\Big| < \varepsilon \quad (6)$$

$$\Big|P\Big(\frac{1}{l} \sum_{k=1}^{l} \xi_{l\cdot(j-1)+k} < t\sqrt{\frac{pq}{l}} + p\Big) - \frac{1}{2\pi} \int_{-\infty}^{t} e^{-\frac{x^2}{2}}\, dx\Big| < \varepsilon. \quad (7)$$

Обозначим

$$y = t\sqrt{\frac{pq}{l}} + p,\ t = (y - p)\sqrt{\frac{l}{pq}}. \quad (8)$$

В этом случае имеем

$$\Big|P\Big(\frac{1}{l} \sum_{k=1}^{l} \xi_{l\cdot(j-1)+k} < y\Big) - \frac{1}{2\pi} \int_{-\infty}^{(y-p)\sqrt{\frac{l}{pq}}} e^{-\frac{x^2}{2}}\, dx\Big| < \varepsilon. \quad (9)$$

Упростим интеграл

$$\frac{1}{2\pi} \int_{-\infty}^{(y-p)\sqrt{\frac{l}{pq}}} e^{-\frac{x^2}{2}}\, dx = \begin{vmatrix} x = (z-p)\sqrt{\frac{l}{pq}} & dx = \sqrt{\frac{l}{pq}}\, dz \\ x = (y-p)\sqrt{\frac{l}{pq}} & z = y \\ x = -\infty & z = -\infty \end{vmatrix} =$$

$$= \frac{1}{2\pi} \sqrt{\frac{l}{pq}} \int_{-\infty}^{y} e^{-\frac{(z-p)^2}{2\left(\sqrt{\frac{pq}{l}}\right)^2}}\, dz. \quad (10)$$

Окончательно имеем

$$\Big|P\Big(\frac{1}{l} \sum_{k=1}^{l} \xi_{l\cdot(j-1)+k} < y\Big) - \frac{1}{2\pi\sqrt{\frac{pq}{l}}} \int_{-\infty}^{y} e^{-\frac{(z-p)^2}{2\left(\sqrt{\frac{pq}{l}}\right)^2}} dz\Big| < \varepsilon. \quad (11)$$

Доказали, что для всех возможных, $1 \le j \le \frac{n}{l}$ функция распределения случайной величины $\zeta_j = \frac{1}{l}\sum_{k=1}^{l} \xi_{l\cdot(j-1)+k}$ равномерно сходится к нормальной случайной величине с математическим ожиданием $m = p$ и дисперсией $\sigma^2 = \frac{pq}{l}$. То есть можно считать, что случайная величина $\zeta_j = \frac{1}{l}\sum_{k=1}^{l} \xi_{l\cdot(j-1)+k}$ является нормальной случайной величиной с математическим ожиданием p и дисперсией $\sigma^2 = \frac{pq}{l}$.

Оценка математического ожидания с помощью распределения Стьюдента

Далее, наша задача – оценить математическое ожидание нормальной случайной величины ζ_j. Напомним определение.

Определение 8. Распределение τ с плотностью вероятности

$$f_\tau(t) = \Big(\frac{1}{\sqrt{\pi n}} \frac{\Gamma(\frac{n+1}{2})}{\Gamma(\frac{n}{2})} (1 + \frac{t^2}{n}\Big)^{-\frac{n+1}{2}}, \quad (12)$$

называется распределением Стьюдента с n степенями свободы. Символом $\Gamma(x)$ обозначена гамма функция

$$\Gamma(k) = \int_{\infty}^{0} t^{k-1} \exp(-t)\, dt, \quad (13)$$

определенная для всех $k > 0$.

Далее, будем пользоваться обозначениями

$$\bar{\zeta} = \frac{1}{l} \sum_{k=1}^{l} \zeta_k \text{ и } \bar{\theta}^2 = \frac{1}{l} \sum_{k=1}^{l} \zeta_k^2 - l(\bar{\zeta})^2 \quad (14)$$

Согласно [1], случайная величина

$$\tau = \frac{\sqrt{l}\,(\bar{\zeta} - m)}{\sqrt{\frac{n\bar{\theta}^2}{l-1}}} = \sqrt{l-1}\,\frac{(\bar{\zeta} - m)}{\bar{\theta}} \quad (15)$$

имеет распределение Стьюдента с $l - 1$ степенями свободы, или

$$P(t_1 < \sqrt{l-1}\,\frac{(\bar{\zeta} - m)}{\bar{\theta}} < t_2) = \int_{t_1}^{t_2} f_\tau(x)\, dx. \quad (16)$$

Или то же самое утверждение. Для плотности вероятности f_τ случайной величины τ с $l - 1$ степенями свободы справедливо равенство

$$P\Big(\bar{\zeta} - \frac{\bar{\theta} t_2}{\sqrt{n-1}} < m < \bar{\zeta} - \frac{\bar{\theta} t_1}{\sqrt{n-1}}\Big) = \int_{t_1}^{t_2} f_\tau(x)\, dx \quad (17)$$

То есть за счет выбора n для любых значений t_1 и t_2 можно сделать величину $\gamma = \int_{t_1}^{t_2} f_\tau(x)\, dx$ сколь угодно близкой к единице. Далее, за счет выбора t_1 и t_2 сделать интервал $[\bar{\zeta} - \frac{\bar{\theta} t_2}{\sqrt{n-1}} < m < \frac{\bar{\theta} t_1}{\sqrt{n-1}}]$ сколь угодно малой длины. И окончательно сделаем вывод – с вероятностью γ величина p лежит на отрезке $[\bar{\zeta} - \frac{\bar{\theta} t_2}{\sqrt{n-1}} < m < \frac{\bar{\theta} t_1}{\sqrt{n-1}}]$.

Окончательно выбираем для каждой r уязвимости свое значение p_r и находим:

$$p = \max_r(p_r). \quad (18)$$

Если $p > p_0$, где p_0 – некоторое заранее определенное число, то система должна прекратить свое функционирование.

Пример

Пусть проводится 1000 испытаний системы на уязвимость. В результате получим 1000 независимых дискретных случайных величин

$$\xi_i = \begin{cases} 1, \text{ система не отреагировала на атаку} \\ 0, \text{ система отреагировала на атаку} \end{cases} \quad (19)$$

Далее, разобьём все испытания на непересекающиеся классы по 100 элементов в каждом и посмотрим сколько раз в каждом классе система отреагировала на атаку. Пусть получена таблица 1, согласно

Таблица 1.

Испытания на непересекающиеся классы по 100 элементов в каждом

классы	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
реакции	53	48	74	26	35	66	79	81	95	18

Таблица 2.

Нормальные случайные величины с их значениями

случайная величина	ζ_1	ζ_2	ζ_3	ζ_4	ζ_5	ζ_6	ζ_7	ζ_8	ζ_9	ζ_{10}
значение сл. величин	0,53	0,48	0,74	0,26	0,35	0,66	0,79	0,81	0,95	0,18

которой, система в первом классе 53 раза не отреагировала на атаку, в втором классе 48 раз не отреагировала на атаку и так далее.

То есть случайные величины ξ_i, $i = 1, \dots, 100$ приняли значение 1 ровно 53 раза и значение 0 ровно 47 раз.

Также случайные величины ξ_i, $i = 101, \dots, 200$ приняли значение 1 ровно 48 раз и значение 0 ровно 52 раза, и так далее.

Как доказано в работе, случайные величины $\zeta_j = \frac{1}{100}\sum_{k=1}^{100}\xi_{100\cdot(j-1)+k}$ можно считать нормальными случайными величинами. В итоге получим таблицу 2:

Введем случайные величины

$$\bar{\zeta} = \frac{1}{10}\sum_{k=1}^{10}\zeta_k = \frac{1}{10}(0{,}53 + 0{,}48 + 0{,}74 + 0{,}26 + 0{,}35 + 0{,}66 + 0{,}79 + 0{,}81 + 0{,}95 + 0{,}18) = 0{,}575$$

$$\bar{\theta}^2 = \frac{1}{10}\sum_{k=1}^{10}\zeta_k^2 - (\bar{\zeta}) = \frac{1}{10}(0{,}53^2 + 0{,}48^2 + 0{,}74^2 + 0{,}26^2 + + 0{,}35^2 + 0{,}66^2 + 0{,}79^2 + 0{,}81^2 + 0{,}95^2 + 0{,}18^2) - 0{,}575^2 = \frac{1}{10}(0{,}2809 + 0{,}2304 + 0{,}5476 + 0{,}0676 + 0{,}1225 + 0{,}4356 + 0{,}6241 + 0{,}6561 + + 0{,}9025 + 0{,}0324) - 0{,}575^2 = 0{,}38997 - 0{,}330625 = 0{,}059345. \quad (20)$$

Согласно [1], случайная величина

$$\tau = \sqrt{l-1}\,\frac{(\bar{\zeta} - m)}{\bar{\theta}} = \sqrt{10-1}\,\frac{0{,}575 - m}{\sqrt{0{,}059345}} = 12{,}31(0{,}575 - m) \quad (21)$$

имеет распределение Стьюдента с 9 степенями свободы, или,

$$P(0{,}575 - 0{,}0812t_2 < m < 0.575 - 0.0812t_1) = \int_{t_1}^{t_2} f_\tau(x)dx.$$

По таблицам для $\gamma = 0{,}95$ из неравенства $\int_{t_1}^{t_2} f_\tau(x)dx > \gamma$ выбираем $t_1 = 0{,}12$ и $t_2 = 0{,}83$. В итоге получим,

$$P(0{,}508 < m < 0{,}584) > 0{,}95. \quad (22)$$

Удобно выбрать $m = 0{,}58$.

Аналогично, проверяя уязвимость различных параметров, получим, например, набор $m_1 = 5{,}8$; $m_2 = 4{,}3$; $m_3 = 7{,}3$; $m_4 = 5{,}9$; $m_5 = 8{,}8$.

Если выбрали $m = 0{,}9$, то из неравенства $0{,}9 = m > m_5 = 8{,}8$ вытекает, что систему необходимо отправить на доработку.

Вывод

В конце работы хотелось бы добавить, что любая величина математического ожидания, лежащая на отрезке $[\bar{\zeta} - \frac{\bar{\theta}t_2}{\sqrt{n-1}} < m < \frac{\bar{\theta}t_1}{\sqrt{n-1}}]$ с вероятностью γ является наилучшим значением математического ожидания с заданной вероятностью находящейся на нашем отрезке, так как распределение Стьюдента, используемое для решения поставленной задачи, здесь используется как точное распределение.

Число p выбирают из соображений, чтобы после запятой было как можно меньше десятичных знаков, или для удобства дальнейших вычислений.

Вычислительный эксперимент наглядно показал, как пользоваться математическим аппаратом и какие выводы можно сделать.

Литература

1. Об отдельных аспектах стандартизации и условий функционирования автоматизированных систем / А.О. Ефимов, И.И. Лившиц, М.О. Мещеряков [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. – 2023. – Т. 50, № 4. – С. 101–108. – DOI 10.21822/2073-6185-2023-50-4-101-108.
2. Левшун Д.С., Веснин Д.В., Котенко И.В. Прогнозирование категорий уязвимостей в конфигурациях устройств с помощью методов искусственного интеллекта //Вопросы кибербезопасности. – 2024. – №. 3. – С. 33–39. DOI: 10.21681/2311-3456-2024-3-33-39.
3. Дровникова, И.Г. Основные виды уязвимостей и взаимосвязь компонентов безопасности при обосновании показателей надёжности системы защиты информации от несанкционированного доступа в автоматизированных системах / И.Г. Дровникова, А.С. Етепнев, Е.А. Рогозин // Приборы и системы. Управление, контроль, диагностика. – 2019. – № 3. – С. 59–64.
4. Ефимов, А.О. Оценка уровня защищенности (безопасности функционирования) автоматизированных систем на основе их уязвимостей, формализованная при помощи теории систем массового обслуживания / А.О. Ефимов, Е.А. Рогозин // Вестник

Дагестанского государственного технического университета. Технические науки. – 2023. – Т. 50, № 2. – С. 83–89. – DOI 10.21822/2073-6185-2023-50-2-83-89
5. Беззатеев С.В. и др. Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности //Научно-технический вестник информационных технологий, механики и оптики. – 2021. – Т. 21. – №. 4. – С. 553–561. DOI: 10.17586/2226-1494-2021-21-4-553-561.
6. Xie H.A comprehensive review on the application of CVSS 4.0 and deep learning in vulnerability //Applied and Computational Engineering. – 2024. – Т. 87. – С. 234–240. DOI:10.54254/2755-2721/87/20241621.
7. Lala S.K., Kumar A., Subbulakshmi T. Secure web development using owasp guidelines //2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS). – IEEE, 2021. – С. 323–332. DOI: 10.1109/ICICCS51141.2021.9432179.
8. Карты источников, содержащих сведения об уязвимостях программного обеспечения / А.Л. Сердечный, М.А. Тарелкин, А.А. Ломов, К.В. Симонов // Информация и безопасность. – 2019. – Т. 22, № 3. – С. 411–422.
9. К вопросу анализа нормативно-правовых документов по информационной безопасности автоматизированных систем органов внутренних дел Российской Федерации для оценки уровня их защищенности / Е.А. Рогозин, И.Г. Дровникова, А.О. Ефимов, В.Р. Романова // Вестник Дагестанского государственного технического университета. Технические науки. – 2022. – Т. 49, № 4. – DOI 10.21822/2073-6185-2022-49-4-97-103.
10. Дровникова, И.Г. Способы оценки уровня защищенности программного обеспечения автоматизированных систем органов внутренних дел и направления их совершенствования / И. Г. Дровникова, А. Д. Попова // Вестник Дагестанского государственного технического университета. Технические науки. – 2023. – Т. 50, № 4. – С. 85–92. – DOI 10.21822/2073-6185-2023-50-4-85-92. – EDN LDTFDM.
11. Концептуальные основы оценки уровня защищенности автоматизированных систем на основе их уязвимости / А.О. Ефимов, И.И. Лившиц, Т.В. Мещерякова, Е.А. Рогозин // Безопасность информационных технологий. – 2023. – Т. 30, № 2. – С. 63–79. – DOI 10.26583/bit.2023.2.04.
12. Вареница В.В. и др. Практические аспекты выявления уязвимостей при проведении сертификационных испытаний программных средств защиты информации //Вопросы кибербезопасности. – 2021. – №. 5 (45). – С. 36–44. DOI:10.21681/2311-3456-2021-5-36-44.
13. Chakraborty S. et al. Deep learning based vulnerability detection: Are we there yet? //IEEE Transactions on Software Engineering. – 2020. – Т. 48. – №. 9. – С. 3280–3296. DOI:10.48550/arXiv.2009.07235.
14. Li Y., Wang S., Nguyen T.N. Vulnerability detection with fine-grained interpretations //Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. – 2021. – С. 292–303. DOI: 10.1145/3468264.3468597.
15. Lin G., Wen S., Han Q.-L., Zhang J. and Xiang Y. Software Vulnerability Detection Using Deep Neural Networks: A Survey in Proceedings of the IEEE. Oct. 2020, vol. 108, no. 10, p. 1825–1848. DOI: DOI: 10.1109/JPROC.2020.2993293.
16. Преображенский, Ю.П. О проблемах защиты данных в информационных системах / Ю.П. Преображенский, О.Н. Чопоров, Е. Ружицкий // Вестник Воронежского института высоких технологий. – 2021. – № 1(36). – С. 70–73.
17. Хорев, А.А. Анализ возможности реализации угроз безопасности информации, обрабатываемой средствами вычислительной техники, с использованием радиомодулей / А.А. Хорев, А.А. Чумаков // Вестник УрФО. Безопасность в информационной сфере. – 2023. – № 4(50). – С. 77–88. – DOI 10.14529/secur230408.
18. Лившиц И.И. Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов / И.И. Лившиц // Труды СПИИРАН. – 2020. – Т. 19, № 2. – С. 383–411. – DOI 10.15622/sp.2020.19.2.6.
19. Проблемные вопросы информационной безопасности киберфизических систем / Д.С. Левшун, Д.А. Гайфулина, А.А. Чечулин, И.В. Котенко // Информатика и автоматизация. – 2020. – Т. 19, № 5. – С. 1050–1088. – DOI 10.15622/ia.2020.19.5.6.
20. Методики оценивания надежности систем защиты информации от несанкционированного доступа в автоматизированных системах / О.И. Бокова, И.Г. Дровникова, А.С. Етепнев [и др.] // Труды СПИИРАН. – 2019. – Т. 18, № 6. – С. 1301–1332. – DOI 10.15622/sp.2019.18.6.1301-1332.
21. Способ расчета времени подготовки возвращаемых блоков ракет космического назначения к последующим пускам / С.Ф. Стельмах, А.М. Астанков, А.Н. Суворов, Н.С. Демидова // Труды МАИ. – 2024. – № 138.

VULNERABILITY ASSESSMENT OF AUTOMATED SYSTEMS USING PROBABILITY THEORY, STUDENT'S DISTRIBUTION, AND NORMAL RANDOM VARIABLES

Atlasov I. V.[11], Efimov A. O.[12], Rogozin E. A.[13], Cherkasova A. S.[14]

Keywords: *mathematical modeling, statistical methods, uncertainty reduction, quantitative indicators, information security, risk analysis, automated systems.*

Purpose of the study: *the study of indicators and mathematical methods for assessing vulnerabilities of automated systems. Consideration of the applicability of probability theory, Student's distribution, and normal random variables in order to comprehensively assess vulnerabilities.*

11 Igor V. Atlasov, Dr. Sc., Professor, Federal State Public Educational Establishment of Higher Training «The Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia», Moscow. E-mail: atlasov.igor.777@gmail.com
12 Alexey O. Efimov, Federal State Public Educational Establishment of Higher Training «Voronezh Institute of the Ministry of the Interior of the Russian Federation», Voronezh. E-mail: ea.aleksei@yandex.ru
13 Evgeny A. Rogozin, Dr.Sc., Professor, Federal State Public Educational Establishment of Higher Training «Voronezh Institute of the Ministry of the Interior of the Russian Federation», Voronezh. evgenirogozin@yandex.ru
14 Anastasia S. Cherkasova, Federal State Public Educational Establishment of Higher Training «Voronezh Institute of the Ministry of the Interior of the Russian Federation», Voronezh. E-mail: cherkasova.30@yandex.ru

Methods of research: *probability theory, Student's distributions, and normal random variables. The object of the study is an automated system with quantitative indicators (in terms of the number of components and the number of vulnerabilities in them).*

Result(s): *the obtained mathematical models of vulnerability assessment significantly reduce the level of uncertainty associated with determining the criticality of threats and their likelihood. The use of statistical methods such as probability theory and Student's distribution allows for a more objective and reproducible assessment of vulnerabilities, excluding subjective factors from the process. In particular, the use of such methods helps to take into account various variations in vulnerability parameters, such as the likelihood of their exploitation, possible consequences and risks, which makes the process more accurate and data-driven. This is especially important in situations where it is necessary to work with limited or incomplete data, such as when evaluating new or subtle vulnerabilities.*

In addition, these models contribute to a significant reduction in the influence of the human factor, which is critical to ensure the objectivity and stability of the assessment. While expert assessment is an important element in traditional analysis methods, mathematical models minimize the need for subjective decisions, which in turn increases accuracy and reduces the likelihood of errors caused by personal interpretation of data. As a result, the use of such models leads to a more automated and objective vulnerability assessment process, which contributes to improved information security risk management and increased security of automated systems.

Scientific novelty: *it consists in the application of probability theory, Student's distribution and normal random variables in order to reduce uncertainty in assessing the vulnerabilities of automated systems. The proposed models, unlike existing ones, allow the use of numerical indicators obtained experimentally, unlike methods (for example, CVSS) using expert assessment.*

References

1. Efimov A.O., Livshits I.I., Meshcheryakov M.O., et al. On certain aspects of standardization and operating conditions of automated systems // Vestnik of Dagestan State Technical University. Technical Sciences. – 2023. – Vol. 50, No. 4. – P. 101–108. – DOI 10.21822/2073-6185-2023-50-4-101-108.
2. Levshun D.S., Vesnin D.V., Kotenko I.V. Forecasting vulnerability categories in device configurations using artificial intelligence methods // Cybersecurity Issues. – 2024. – No. 3. – P. P. 33–39. DOI: 10.21681/2311-3456-2024-3-33-39.
3. Drovdnikova I.G., Etepnev A.S., Rogozin E.A. Main types of vulnerabilities and interrelation of security components in substantiating reliability indicators of information protection systems against unauthorized access in automated systems // Devices and Systems. Control, Monitoring, Diagnostics. – 2019. – No. 3. – P. 59–64.
4. Efimov A.O., Rogozin E.A. Assessment of the security level (operational safety) of automated systems based on their vulnerabilities, formalized using the queuing theory // Vestnik of Dagestan State Technical University. Technical Sciences. – 2023. – Vol. 50, No. 2. – P. 83–89. – DOI 10.21822/2073-6185-2023-50-2-83-89.
5. Bezzateev S.V., et al. Risk assessment methodology for information systems based on user behavior analysis and information security incidents // Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics. – 2021. – Vol. 21, No. 4. – P. 553–561. DOI: 10.17586/2226-1494-2021-21-4-553-561.
6. Xie H.A comprehensive review on the application of CVSS 4.0 and deep learning in vulnerability analysis // Applied and Computational Engineering. – 2024. – Vol. 87. – P. 234–240. DOI:10.54254/2755-2721/87/20241621.
7. Lala S.K., Kumar A., Subbulakshmi T. Secure web development using OWASP guidelines // 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS). – IEEE, 2021. – P. 323–332. DOI: 10.1109/ICICCS51141.2021.9432179.
8. Serdechny A.L., Tarelkin M.A., Lomov A.A., Simonov K.V. Source maps containing information on software vulnerabilities // Information and Security. – 2019. – Vol. 22, No. 3. – P. 411–422.
9. Rogozin E.A., Drovdnikova I.G., Efimov A.O., Romanova V.R. On the analysis of regulatory documents on information security of automated systems of the Ministry of Internal Affairs of the Russian Federation for assessing their security level // Vestnik of Dagestan State Technical University. Technical Sciences. – 2022. – Vol. 49, No. 4. – P. 97–103. – DOI 10.21822/2073-6185-2022-49-4-97-103.
10. Drovdnikova I.G., Popova A.D. Methods for assessing the security level of software for automated systems of the Ministry of Internal Affairs and directions for their improvement // Vestnik of Dagestan State Technical University. Technical Sciences. – 2023. – Vol. 50, No. 4. – P. 85–92. – DOI 10.21822/2073-6185-2023-50-4-85-92.
11. Efimov A.O., Livshits I.I., Meshcheryakova T.V., Rogozin E.A. Conceptual foundations for assessing the security level of automated systems based on their vulnerabilities // Information Technology Security. – 2023. – Vol. 30, No. 2. – P. 63–79. – DOI 10.26583/bit.2023.2.04.
12. Varenitsa V.V., et al. Practical aspects of vulnerability detection in the certification testing of information protection software // Cybersecurity Issues. – 2021. – No. 5 (45). – P. 36–44. DOI:10.21681/2311-3456-2021-5-36-44.
13. Chakraborty S., et al. Deep learning-based vulnerability detection: Are we there yet? // IEEE Transactions on Software Engineering. – 2020. – Vol. 48, No. 9. – P. 3280–3296. DOI:10.48550/arXiv.2009.07235.
14. Li Y., Wang S., Nguyen T. N. Vulnerability detection with fine-grained interpretations // Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. – 2021. – P. 292–303. DOI: 10.1145/3468264.3468597.
15. Lin, G., Wen, S., Han, Q.-L., Zhang, J., and Xiang, Y. Software Vulnerability Detection Using Deep Neural Networks: A Survey in Proceedings of the IEEE. Oct. 2020, vol. 108, no. 10, p. 1825–1848. DOI: 10.1109/JPROC.2020.2993293.

16. Preobrazhensky Yu. P., Choporov O. N., Ruzhitsky E. On data protection issues in information systems // Vestnik of Voronezh Institute of High Technologies. – 2021. – No. 1(36). – P. 70–73.
17. Khorev A. A., Chumakov A. A. Analysis of the possibility of implementing security threats to information processed by computing devices using radio modules // Vestnik UrFO. Security in the Information Sphere. – 2023. – No. 4(50). – P. 77-88. – DOI 10.14529/secur230408.
18. Livshits I. I. Security assessment method for cloud IT components based on existing standards // SPIIRAS Proceedings. – 2020. – Vol. 19, No. 2. – P. 383–411. – DOI 10.15622/sp.2020.19.2.6.
19. Levshun D. S., Gaifullina D. A., Chechulin A. A., Kotenko I. V. Problematic issues of cybersecurity in cyber-physical systems // Informatics and Automation. – 2020. – Vol. 19, No. 5. – P. 1050–1088. – DOI 10.15622/ia.2020.19.5.6.
20. Bokova O. I., Drovdnikova I. G., Etepnev A. S., et al. Methods for assessing the reliability of information protection systems against unauthorized access in automated systems // SPIIRAS Proceedings. – 2019. – Vol. 18, No. 6. – P. 1301–1332. – DOI 10.15622/sp.2019.18.6.1301-1332.
21. Stelmakh S. F., Astankov A. M., Suvorov A. N., Demidova N. S. Method for calculating the preparation time of reusable rocket blocks for subsequent launches // MAI Proceedings. – 2024. – No. 138.