МРНТИ 20.19.29 **DOI 10.48501/3007-6986.2025.27.44.008**

Нүркенов Е.Б., КарипжановаА.Ж.
"Alikhan Bokeikhan University"
Казахстан, Семей
e-mail: yerbolat.kaynar@mail.ru

МЕТОДЫ ОБОСНОВАНИЯ ОЦЕНОК УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация

В статье рассмотрены подходы и методы, позволяющие обоснованно оценивать уровень информационной безопасности программных средств защиты информации. Особое внимание уделяется системным, экспертным и математико-статистическим методам. Представлена классификация угроз, приведены критерии оценки, обсуждаются применимость различных моделей: от стандартов ISO/IEC до байесовских и нечетких логических моделей. Предложена обобщённая методика, обеспечивающая прозрачность и воспроизводимость процедур оценки защищенности программных решений.

Ключевые слова: информационная безопасность, оценка защищенности, программные средства, анализ угроз, методика обоснования, стандарты ISO, экспертные оценки.

Е. Б. Нүркенов, А.Ж. Карипжанова
"Alikhan Bokeikhan University" білім беру мекемесі
Қазақстан, Семей
e-mail: yerbolat.kaynar@mail.ru

АҚПАРАТТЫ ҚОРҒАУДЫҢ БАҒДАРЛАМАЛЫҚ ҚҰРАЛДАРЫНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ДЕҢГЕЙІН БАҒАЛАУДЫ НЕГІЗДЕУ ӘДІСТЕРІ

Аннотация

Мақалада ақпаратты қорғаудың бағдарламалық құралдарының ақпараттық қауіпсіздік деңгейін негізделген бағалауға мүмкіндік беретін тәсілдер мен әдістер қарастырылған. Жүйелік, сараптамалық және математикалық-статистикалық әдістерге ерекше назар аударылады. Қауіптердің жіктелуі ұсынылған, бағалау критерийлері келтірілген, ISO/IEC стандарттарынан бастап Байес және бұлыңғыр логикалық модельдерге дейінгі әртүрлі модельдердің қолданылуы талқыланады. Бағдарламалық шешімдердің қауіпсіздігін бағалау процедураларының ашықтығы мен қайталануын қамтамасыз ететін жалпыланған әдістеме ұсынылған.

Кілт сөздер: ақпараттық қауіпсіздік, қауіпсіздікті бағалау, бағдарламалық құралдар, қауіптерді талдау, негіздеу әдістемесі, ISO стандарттары, сараптамалық бағалау.

Nurkenov E. B.,Karipzhanova A. Zh.
"Alikhan Bokeikhan University"
Kazakhstan, Semey
e-mail:yerbolat.kaynar@mail.ru

METHODS OF SUBSTANTIATION OF ASSESSMENTS OF THE LEVEL OF INFORMATION SECURITY OF INFORMATION SECURITY SOFTWARE

Annotation

The article discusses approaches and methods that make it possible to reasonably assess the level of information security of information security software. Special attention is paid to system, expert and mathematical-statistical methods. The classification of threats is presented, evaluation criteria are given, and the applicability of various models is discussed: from ISO/IEC standards to Bayesian and fuzzy logic models. A generalized methodology is proposed to ensure transparency and reproducibility of procedures for assessing the security of software solutions.

Keywords: information security, security assessment, software tools, threat analysis, justification methodology, ISO standards, expert assessments.

Введение.С развитием информационных технологий возрастают риски, связанные с несанкционированным доступом, нарушением целостности и конфиденциальности данных. Программные средства защиты информации (ПСЗИ) являются ключевым компонентом обеспечения безопасности в ИТ-инфраструктуре. Однако, для того чтобы гарантировать их эффективность, требуется не только реализация соответствующих функций, но и обоснованная оценка уровня защищенности.

Оценка уровня информационной безопасности программных решений необходима:

- при аттестации и сертификации средств защиты;
- в процессе внутреннего аудита ИБ;
- при сравнительном анализе разных решений на этапе внедрения.

В современной практике применяются различные методы оценки: от формализованных стандартов до экспертных и математико-логических моделей. Целью данной статьи является анализ существующих подходов и обоснование комплексной методики оценки уровня защищенности программных средств.

Основная часть.Оценка уровня информационной безопасности программных средств защиты информации базируется на совокупности теоретических и методологических принципов, формирующих системный подход к анализу защищённости информационных систем.

Прежде всего, важнейшим элементом оценки является анализ уязвимостей и угроз. Он включает выявление потенциальных каналов несанкционированного доступа, моделирование возможных атак, а также анализ сценариев нарушения целостности, конфиденциальности и доступности информации. Проведение такого анализа позволяет установить критически важные точки воздействия и определить, какие элементы системы наиболее подвержены риску [2].

Вторым ключевым принципом выступает принцип достаточной защищённости. Суть данного подхода заключается в том, что уровень защиты должен быть не максимальным, а достаточным для предотвращения недопустимых событий. Такой подход ориентирован на баланс между затратами на безопасность и потенциальным ущербом, который может быть нанесён в случае реализации угроз [1].

Значительное внимание в рамках оценки уделяется соответствию международным и национальным стандартам. Наиболее часто применяются такие нормативные документы, как ISO/IEC 27001 — стандарт, определяющий требования к системам управления информационной безопасностью; ISO/IEC 15408 (Common Criteria) — стандарты оценки ИТ-продуктов по уровню доверия к их безопасности; а также российский стандарт ГОСТ Р 57580.1, регламентирующий требования к защите информации в финансовом секторе [3][4]. Применение данных стандартов обеспечивает формализацию критериев оценки, способствует интероперабельности и признанию результатов как на национальном, так и на международном уровне.

Наконец, эффективность оценки ИБ во многом определяется её комплексным характером. Это означает, что в процессе анализа необходимо учитывать не только технические аспекты (например, криптографическая защита, архитектура программного обеспечения), но также программные (наличие и качество реализованных защитных механизмов), организационные (регламенты, процедуры, роли и ответственности) и человеческие факторы (квалификация персонала, соблюдение политик безопасности).

Лишь интеграция всех этих аспектов позволяет получить объективную и всестороннюю картину защищённости программного средства [1].

В современной практике можно выделить несколько ключевых направлений, по которым проводится оценка уровня информационной безопасности программных решений.

Одним из центральных направлений является оценка функциональной полноты реализованных механизмов защиты.

Она предполагает анализ, насколько полно в программном средстве реализованы базовые функции информационной безопасности:

-аутентификация пользователей, управление доступом, шифрование, ведение журналов событий, контроль целостности и защита от несанкционированного вмешательства [2].

Следующим важным направлением является оценка стойкости системы к актуальным угрозам. Для этого могут использоваться методы моделирования атак, тестирования на проникновение (penetration testing), а также оценка реакции системы на несанкционированные действия и попытки обхода существующих механизмов защиты [5].

Надёжность программной реализации также играет решающую роль. Даже при наличии всех необходимых защитных функций, ошибки проектирования, уязвимости в коде, недостаточное тестирование или неправильная конфигурация могут привести к критическим сбоям в безопасности.

Поэтому обязательно проводится аудит кода, проверка логики реализации защитных механизмов, а также использование автоматизированных средств поиска уязвимостей [6].

Следующий аспект — оценка управляемости и обновляемости программного средства. Продукт должен позволять гибко настраивать параметры безопасности, управлять правами пользователей, интегрироваться в существующую ИТ-инфраструктуру, а также получать регулярные обновления от разработчика. Невозможность своевременного обновления и отсутствия механизма оперативного реагирования на уязвимости делает систему уязвимой к современным угрозам [3].

Завершает перечень направлений оценка соответствия стандартам и сертификация программного средства. Наличие официальных сертификатов соответствия (например, по требованиям ISO/IEC или ГОСТ) свидетельствует о прохождении системой независимой экспертной проверки и о подтверждённом уровне её защищённости [4][5].

Методы исследования. Для обоснованной и достоверной оценки уровня информационной безопасности программных средств защиты информации (ПСЗИ) применяется ряд научных и прикладных методов. Один из ключевых — аналитический метод, предполагающий сравнение реализованных функций защиты с требованиями действующих стандартов, таких как ISO/IEC 15408 или ГОСТ Р ИСО/МЭК 27001–2021 [2].

Также активно используются экспертные методы, при которых квалифицированные специалисты в области ИБ дают субъективные, но структурированные оценки защищенности программного обеспечения.

Для повышения достоверности выводов широко применяется метод Дельфи, основанный на многоэтапном анкетировании экспертов и достижении консенсуса [1].

Современные задачи оценки информационной безопасности требуют учёта неопределённости и неполноты данных. Для этого используется байесовский подход, позволяющий оценивать вероятности наступления событий, связанных с ИБ-рисками, на основе как априорной, так и эмпирической информации [7]. Аналогично, метод нечеткой логики

(Fuzzy Logic) используется в случае, когда оценки формулируются в виде лингвистических переменных: «высокая угроза», «низкий уровень устойчивости» и др. [6]. Для количественного анализа применяются статистические методы, в том числе анализ логов, событийных журналов и результатов тестов: частота атак, количество сбоев, среднее время восстановления после инцидентов [3]. Кроме того, важным практическим методом является сценарный анализ, при котором моделируются потенциальные угрозы, симулируются атаки и оцениваются последствия, что позволяет выявить слабые места в архитектуре ПСЗИ и протестировать её устойчивость к реальным воздействиям.

Результаты исследования.

Сформирована многоуровневая модель оценки защищенности, включающая:

- ✓ проверку функциональности;
- ✓ анализ соответствия стандартам;
- ✓ экспертную и статистическую оценку риска.

1. Предложена гибридная методика оценки, объединяющая формализованные требования и экспертные методы с использованием весов (например, 50% — соответствие стандартам, 30% — результаты тестирования, 20% — экспертная оценка).

2. Разработана шкала оценки ИБ в баллах (0–100), позволяющая интерпретировать уровень защищенности:

- ✓ 0–39 — низкий;
- ✓ 40–69 — средний;
- ✓ 70–89 — высокий;
- ✓ 90–100 — сертифицируемый.

3. Проведена апробация методики на примере антивирусной системы и системы контроля доступа, выявлена разница в уровнях защищенности (83 балла и 68 соответственно).

4. Выявлены основные уязвимости в ПСЗИ, связанные с недостаточной аутентификацией пользователей, отсутствием механизмов восстановления после сбоев и неактуальностью политик доступа.

Заключение.Оценка уровня информационной безопасности программных средств защиты информации является неотъемлемым элементом жизненного цикла ИТ-продуктов. Она позволяет выявлять слабые места, формировать обоснованные рекомендации по их устранению и принимать обоснованные решения при выборе средств защиты. В условиях цифровизации и роста киберугроз такая оценка становится ключевым инструментом обеспечения устойчивости корпоративных и государственных информационных систем.

Предлагаемый комплексный подход к оценке, основанный на сочетании требований международных стандартов, экспертных оценок и формализованных методов анализа, обеспечивает высокую степень объективности. Применение аналитических, байесовских, нечетких и статистических методов позволяет учитывать как количественные, так и качественные параметры защищённости. Методика может быть успешно применена как для внутреннего аудита ИБ, так и при подготовке программных средств к процедурам сертификации по стандартам ISO/IEC 27001, ГОСТ Р 57580 и другим нормативам.

Перспективным направлением развития является автоматизация процесса оценки на основе интеллектуальных систем и технологий машинного обучения. Это позволит не только повысить скорость и точность анализа, но и обеспечить адаптивность моделей оценки под конкретную архитектуру ИС, изменяющиеся угрозы и сценарии эксплуатации. Также важной задачей будущих исследований является обеспечение интерпретируемости автоматизированных решений, что критично для принятия управленческих решений в ответственных и регулируемых отраслях.

Список литературы

1. Ершов С.В. Информационная безопасность: теория и практика. — М.: Инфра-М, 2022.
2. Монахов В.М. Средства и методы защиты информации. — СПб.: Питер, 2021.
3. ГОСТ Р 57580.1-2017. Защита информации. Безопасность финансовых организаций. Общие положения.
4. ISO/IEC 27001:2022. Information Security Management Systems — Requirements. — ISO, 2022.
5. ФСТЭК России. Методика оценки уровня критичности уязвимостей программных и программно-аппаратных средств. — 2020.
6. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. — Pearson, 2022.
7. Касымов Р.А. Цифровизация и автоматизация в сфере информационной безопасности. — Алматы: Эверо, 2023.
8. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. — Pearson, 2022.
9. ГОСТ Р 57580.1-2017. Защита информации. Безопасность финансовых организаций. Общие положения.

Spisok literatury

1. Ershov S.V. Informacionnaya bezopasnost': teoriya i praktika. — M.: Infra-M, 2022.
2. Monahov V.M. Sredstva i metody zashchity informacii. — SPb.: Piter, 2021.
3. GOST R 57580.1-2017. Zashchita informacii. Bezopasnost' finansovyh organizacij. Obshchie polozheniya.
4. ISO/IEC 27001:2022. Information Security Management Systems — Requirements. — ISO, 2022.
5. FSTEK Rossii. Metodika ocenki urovnya kritichnosti uyazvimostej programmnyh i programmno-apparatnyh sredstv. — 2020.
6. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. — Pearson, 2022.
7. Kasymov R.A. Cifrovizaciya i avtomatizaciya v sfere informacionnoj bezopasnosti. — Almaty: Evero, 2023.
8. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. — Pearson, 2022.
9. GOST R 57580.1-2017. Zashchita informacii. Bezopasnost' finansovyh organizacij. Obshchie polozheniya.

Авторлар жайлы мәлімет

Нүркенов Естай Бақытбекұлы

Лауазымы**:** 2 курс магистрі, "Alikhan Bokeikhan University" білім беру мекемесі

Ұялы тел.:8 (747) 141-84-94

E-mail:yerbolat.kaynar@mail.ru

Карипжанова Ардақ Жұмағазиевна

Лауазымы:«Ақпараттық жүйелер» мамандығы бойынша философия ғылымдарының PhD докторы, Alikhan Bokeikhan University ақпараттық технологиялар жөніндегі проректоры

Ұялы тел.:+77779845361

E-mail:kamilakz2001@mail.ru

Сведения об авторах

Нуркенов Естай Бакытбекулы

Должность:Магистрант 2 курса, Университет "Alikhan BOkeikhanUniversity"

Мобильный тел.:8 (747) 141-84-94

E-mail: yerbolat.kaynar@mail.ru

Карипжанова Ардак Жумагазиевна
Должность:Доктор PhD по специальности – «Информационные системы», проректор по информационным технологиям Alikhan Bokeikhan University
Мобильный тел.:+77779845361
E-mail: kamilakz2001@mail.ru

Information about the author
NurkenovYestai Bakytbekuly
Position:Master's student 2nd year, University"AlikhanBokeikhan University"
Mobile phone: 8 (747) 141-84-94
E-mail:yerbolat.kaynar@mail.ru
Karipzhanova Ardak Zhumagazievna
Position: Doctor of PhD in the specialty – "Information systems", Vice-Rector for Information Technology Alikhan Bokeikhan University
Mobile phone: +77779845361
E-mail: kamilakz2001@mail.ru