УДК: 004.056.5

Алексей О. Ефимов[1], Илья И. Лившиц[2], Татьяна В. Мещерякова[3], Евгений А. Рогозин[4]
[1,3,4]Воронежский институт МВД России,
пр-кт Патриотов, 53, Воронеж, 394065, Россия
[2]Университет ИТМО,
Кронверкский пр-кт, 49, Санкт-Петербург, 197101, Россия.
[1]e-mail: ea.aleksei@yandex.ru, https://orcid.org/0000-0001-7559-8113
[2]e-mail: Livshitz.i@yandex.ru, https://orcid.org/0000-0003-0651-8591
[3]e-mail: tmeshcheriakova4@mvd.ru, https://orcid.org/0009-0007-6453-9549
[4]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОСНОВЕ ИХ УЯЗВИМОСТИ

DOI: http://dx.doi.org/10.26583/bit.2023.2.04

Аннотация. В работе представлены концептуальные основы оценки уровня защищенности автоматизированных систем на основе их уязвимости. Проведен анализ, регламентирующих стандартов, методических рекомендаций и нормативных документов в области оценки и классификации уязвимостей информационных систем. Согласно анализу проекта обновления нормативных документов, сделан вывод о равенстве терминов «автоматизированная система» и «информационная система», что позволяет применять все необходимые требования, рекомендации, формальные описания и прочие стандартизированные требования, применимые к информационным системам. Проведен анализ процесса и причин обнаружения уязвимостей автоматизированной системы. Рассмотрено формирование совокупностей уязвимостей, предложено определение базовой и текущей уязвимости автоматизированной системы, а также рассмотрены пути их эффективного устранения. Рассмотрена методика оценки критичности уязвимостей ФСТЭК России, основанная на международной методике CVSS 3.1. В целях удобства самостоятельного расчета критичности уязвимости проведена адаптация и тщательное описание процесса оценки критичности уязвимости стандарта CVSS 3.1. Предложена методика оценки уровня защищенности путем анализа критичности уязвимости автоматизированной системы (совокупности критичности уязвимостей автоматизированной системы). Представлены выводы о направлении дальнейшего исследования: создание модели оценки защищенности на основе уязвимостей, а также модели прогнозирования уязвимостей.

Ключевые слова: автоматизированная система, уязвимость, оценка защищенности, критичность уязвимости, уровень защищенности, методика оценки уязвимости.
Для цитирования: ЕФИМОВ, Алексей О. и др. КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОСНОВЕ ИХ УЯЗВИМОСТИ. Безопасность информационных технологий, [S.l.], т. 30, № 2, с. 63–79, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1497. DOI: http://dx.doi.org/10.26583/bit.2023.2.04.

Aleksey O. Efimov[1], Ilya I. Livshitz[2], Tatiana V. Meshcherakova[3], Evgeniy A. Rogozin[4]
[1,3,4]Voronezh Institute of the Ministry of Internal Affairs of Russia,
Patriotov Ave., 53, Voronezh, 394065, Russia
[2]ITMO University,
Kronverksky Ave., 49, Saint Petersburg, 197101, Russia
[1]e-mail: ea.aleksei@yandex.ru, https://orcid.org/0000-0001-7559-8113
[2]e-mail: Livshitz.i@yandex.ru, https://orcid.org/0000-0003-0651-8591
[3]e-mail: tmeshcheriakova4@mvd.ru, https://orcid.org/0009-0007-6453-9549
[4]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000- 0002-4455-7535

Conceptual foundations for assessing the level of security of automated systems based on their vulnerability

DOI: http://dx.doi.org/10.26583/bit.2023.2.04

Abstract. The paper presents the conceptual framework for assessing the level of security of automated systems based on their vulnerability. The analysis of regulatory standards, methodological recommendations and regulatory documents in the field of assessment and classification of vulnerabilities of information systems is carried out. According to the analysis of the draft update of regulatory documents, it was concluded that the terms automated system and information system are equal, which allows applying all the necessary requirements, recommendations, formal descriptions, and other standardized requirements applicable to information systems. The analysis of the process and causes of the detection of vulnerabilities of the automated system, the formation of sets of vulnerabilities, the definition of the basic vulnerability of the automated system, and the current vulnerability of the automated system, as well as the ways to eliminate these vulnerabilities are considered. The method of assessing the criticality of vulnerabilities of the FSTEC of Russia, based on the international CVSS 3.1 methodology, is considered. In order to make it easier to independently calculate the criticality of vulnerability, adaptation is made, and a thorough description of the process of assessing the criticality of vulnerability of the CVSS 3.1 standard is made. A methodology for assessing the level of security is proposed by analyzing the criticality of the vulnerability of an automated system (the totality of the criticality of vulnerabilities of an automated system). Conclusions are drawn about the direction of further research: the construction of a security assessment model based on vulnerability, as well as a vulnerability prediction model.

Keywords: automated system, vulnerability, security assessment, vulnerability criticality, security level, vulnerability assessment methodology.

For citation: EFIMOV, Aleksey O. et al. Conceptual foundations for assessing the level of security of automated systems based on their vulnerability. IT Security (Russia), [S.l.], v. 30, no. 2, p. 63–79, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1497. DOI: http://dx.doi.org/10.26583/bit.2023.2.04.

Введение

Стремительный рост развития информационных технологий (ИТ) объективно приводит к возникновению существенного числа совокупностей различного программного и аппаратно-программного обеспечения. В настоящее время невозможно не учитывать версии того или иного продукта как компонента ИТ при создании автоматизированной системы (АС). В целях обеспечения оценки уровня защищенности АС предлагается концепция, основанная на учёте критичности уязвимостей АС.

Объективно, рассмотрение вопросов оценки защищенности АС вызывает необходимость исследования значительного числа аспектов защищенности АС, которые в свою очередь постоянно изменяются в связи с высокой скоростью смены поколений технологий передачи, обработки и хранения информации. Отбрасывание ряда факторов, которые в настоящее время имеют большой вес в вопросах защиты информации, оценки уровня защищенности данных, оценки уровня защищенности средств обработки информации, могут привести к существенным расходам при нарушении целостности системы защиты, а также утрате защищаемой информации.

Принимается во внимание факт того, что в связи с особенностями проблемы оценки защищенности АС через совокупность критичности различного рода уязвимостей, разработка научно закрепленной методологической базы, так или иначе связана с трудностями осуществления учета всех факторов, влияющих на уязвимости АС и отдельных компонент АС. Наиболее существенной из этих особенностей является повышенный интерес злоумышленников к уязвимостям АС. Он связан, прежде всего, с открытой публикацией способов эксплуатации уязвимостей, и тем обстоятельством, что открытие доступа к информации конфиденциального характера может нести в себе реальные денежные, материальные и репутационные потери.

1. Анализ нормативных и иных документов, определяющих понятие уязвимости

Указанная проблема оценки защищенности АС с учетом уязвимости должна рассматриваться как комплексная. В связи с этим, решение должно формироваться путем построения концепции, рассматривающей все актуальные факторы, влияющие на защищенность АС. Принцип системности в качестве основы исследования вопросов защищенности АС в защищенном исполнении, предполагает [1]:

- анализ всех возможных угроз безопасности информации в АС;
- анализ параметров качества (эффективности) функционирования базового комплекта средств защиты информации (СЗИ);
- выбор базового комплекта СЗИ АС по оптимальным значениям параметров их качества (эффективности) функционирования для повышения требуемого уровня защищенности при минимизации негативного влияния базового комплекта СЗИ на эффективность функционирования АС по прямому назначению;
- обеспечение защиты на этапе полного жизненного цикла АС, в том числе и в каждой составной части АС по отдельности;
- оценка критичности уязвимостей АС;
- оценка безопасности обновлений компонент АС в защищенном исполнении.

Для проработки отдельных аспектов теории оценки защищенности АС с учетом уязвимости, проведен общий анализ этих проблем [2].

Определение 1. Под уязвимостью АС следует понимать недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации[1].

Основные цели ИБ известны и определены посредством возлагаемых задач на базовый комплект ЗИ в АС, выполненных в защищенном исполнении. При рассмотрении задачи устранения уязвимостей, как одной из самой первостепенной и основополагающей, цели обеспечения ИБ возможно представить следующим образом:

- защита информации от использования уязвимости в целях кражи информации (конфиденциальность);
- защита информации от использования уязвимости в целях модификации либо подмены информации (целостность);
- защита информации путем недопущения использования уязвимости в целях нарушения работы технических средств обработки и передачи информации (доступность).

Определение 2. Под критичностью уязвимости следует понимать совокупность основных технических характеристик уязвимости ПО, аппаратного обеспечения и встроенного ПО. Эта оценка включает в себя числовую оценку, указывающую на серьезность уязвимости по сравнению с другими уязвимостями.

Системный подход опирается на три основных принципа – целостности, сложности и цели [1]. В соответствии с принципом целостности уязвимость АС рассматривается как нечто целое, имеющее свою динамику развития и свою специфику. Принцип сложности следует из объективной сложности исследования уязвимости АС и процессов ее обнаружения и использования и требует разработки и применения количественных и качественных критериев, характеризующих критичность уязвимости. Принцип цели

[1]ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. М.: Стандартинформ. 2015. – 8 с.

обязывает при исследовании уязвимости АС раскрывать, каким образом реализуется эксплуатация уязвимости.

Системный подход приводит к необходимости дополнительного более обширного анализа ряда аспектов, сопряженных с оценкой критичности уязвимости АС в совокупности применяемых средств и систем [1]. В определенных выше заключениях системный подход определяет ряд основных потоков и стадий деятельности [1]:

1) системное рассмотрение сущности исследуемой проблемы оценки защищенности АС и критичности уязвимости АС;

2) разработка и обоснование полной и непротиворечивой концепции решения проблемы;

3) системное использование методов моделирования исследуемых процессов оценки защищенности АС;

4) результатами решения задач является методика и программно-методический комплекс оценки защищенности АС с учетом уязвимости.

Определение 3. Под системно-комплексным подходом будем понимать все множество взглядов, положений и решений, необходимых и достаточных для всеобъемлющего решения всех задач и проблем, возникающих при комплексной оценке критичности уязвимости АС [1].

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций[2]. Также согласно примечанию проекта обновления соответствующего государственного стандарта[3] термин «автоматизированная система», установленный ГОСТ 34.003, можно считать эквивалентным термину «информационная система». Следует отметить, что в ноябре 2021 г. ГОСТ 34.003-90 «Термины и определения» заменяется на ГОСТ Р 59853-2021 (приказ Росстандарта № 1520-ст от 19.11.2021)[4], но в целом существенных изменений в рассматриваемой области терминологии не определено.

Компонент информационной системы – часть информационной системы, включающая некоторую совокупность информации и обеспечивающих её обработку отдельных информационных технологий и технических средств[1].

Под уязвимостью технических средств подразумеваются уязвимости микропрограмм в постоянных запоминающих устройствах, уязвимости микропрограмм в программируемых логических интегральных схемах, уязвимости базовой системы ввода-вывода, уязвимости ПО контроллеров управления, интерфейсов управления и другие уязвимости, иные уязвимости технических средств[1].

Уязвимости, вызванные конфликтом взаимодействия средств и систем защиты информации: ошибки программирования, недостатки, связанные с возможностью обхода, отключения, преодоления функций безопасности и другие уязвимости, определенные несовместимостью используемых средств защиты.

В [3] определено, что уязвимость является составной частью описания угрозы безопасности информации, и отсутствие указания на уязвимость делает неопределенным описание способа реализации угрозы, а значит и самой угрозы [3]. Из вышеприведенного, можно сделать вывод, что реализация угроз возможна лишь при наличии не устранённых

[2]ГОСТ Р 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные. системы. Автоматизированные системы. Термины и определения. 1992. – 26 с.
[3]ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. 2000. – 14 с.
[4]ГОСТ Р 59853-2021 Автоматизированные системы. Термины и определения. 2021. – 12 с.

уязвимостей. Также понятие уязвимости определено в соответствующем международном стандарте[5] – слабость актива или нескольких видов активов, которые могут быть использованы одной или более угрозами, что также подтверждает важность наличия уязвимости при реализации угроз ИБ [4–5].

В целях оценки уровня защищенности, предлагается рассмотрение уязвимостей АС в их совокупности в комплексе. Причины возникновения уязвимостей разнообразны, но определенно важно учитывать их наличие на этапе проектирования систем [6–9]. Применение заведомо скомпрометированного и/или устаревшего набора программных и технических средств может привести к принципиально большому числу уязвимостей, а также их высокой оценки критичности. В связи с этим предполагается, что на этапе проектирования АС будут подбираться совместимые между собой компоненты, которые поддерживаются разработчиком, и в совокупности применяемых средств не имеют наличия не устранённых критичных уязвимостей.

2. Рассмотрение проблемы совокупности уязвимостей

В целях формирования величины уязвимости системы по завершению проектирования и введения системы в эксплуатацию, предлагается ввести определение **базовой уязвимости АС** – это совокупность обнаруженных и не устранённых уязвимостей, вводимой в эксплуатацию АС, удовлетворяющей по критерию критичности существующих уязвимостей (допустимых уязвимостей). Схема формирования базовой уязвимости АС представлена на рис. 1.

Рис. 1. Схема формирования базовой уязвимости АС
Fig. 1. Diagram of the formation of the basic vulnerability of the AS

Устранение уязвимостей АС может производиться разработчиком конкретных программных и/или аппаратных продуктов посредством выпуска обновлений и патчей безопасности. Отдельное внимание должно уделяться правильности применения этих видов устранения уязвимостей. Неправильная установка, либо несоблюдение требований

[5]ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

к установке, может повлечь дополнительные риски к увеличению числа уязвимостей данного продукта. Устранение уязвимостей системами и средствами ЗИ, также предполагает постоянное поддержание их в актуальном состоянии. Также допускается, применение организационных ограничений, либо настройка и управление настройками и политиками безопасности, в целях устранения некоторого числа известных уязвимостей АС. Схема устранения базовой уязвимости АС представлена на рис. 2.

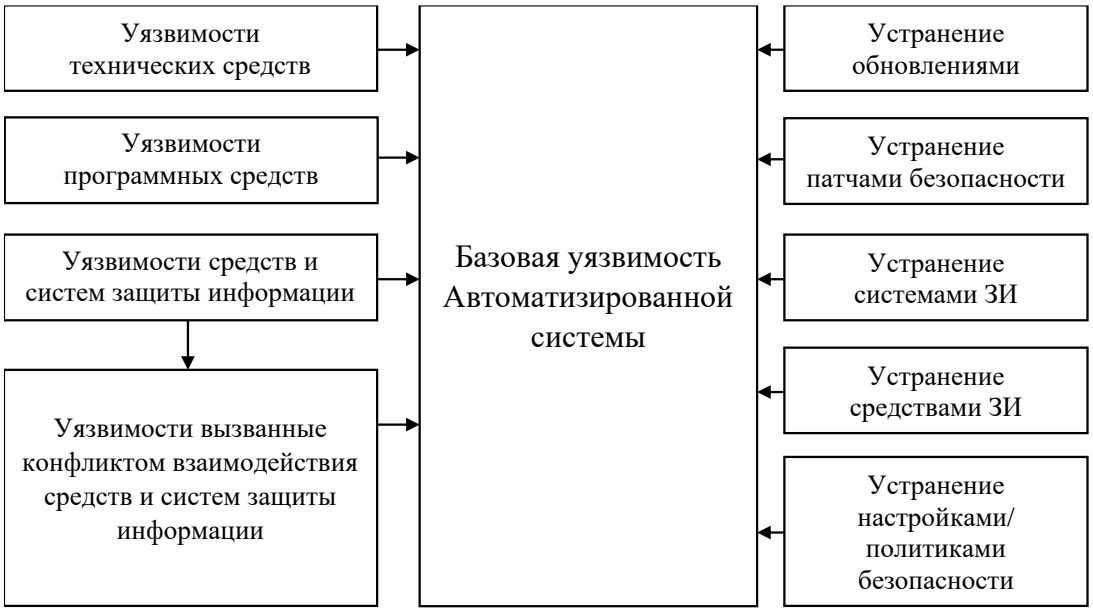

Рис. 2. Схема устранения базовой уязвимости АС
Fig. 2. Scheme of elimination of the basic vulnerability of the AS

По вводу системы в эксплуатацию, необходимо также регулярно проводить проверку АС на наличие новых уязвимостей системы. Как правило, чем больше распространение продукта, тем больше обнаруживается уязвимостей, но, с другой стороны, ресурсы разработчиков позволяют в кратчайшие сроки проводить обновления безопасности. Исходя из этого предполагается, что уязвимости в том либо ином виде присутствуют во всех программных и/или программно-аппаратных продуктах, но обнаруживаются далеко не всегда как злоумышленниками, так и «белыми» хакерами [10–13]. Как показывает статистика зарегистрированных уязвимостей, начиная с 2017 г., идет существенный рост числа обнаруживаемых уязвимостей[6] [14]. Диаграмма числа обнаруженных уязвимостей в АС представлена на рис. 3.

Так как в процессе эксплуатации могут обнаруживаться дополнительные уязвимости АС, то для рассмотрения их в комплексе, предлагается ввести понятие **текущей уязвимости** – это совокупность обнаруженных не устранённых уязвимостей АС в текущий момент времени. Схема формирования текущей уязвимости АС показана на рис. 4.

[6]Common Vulnerabilities and Exposures. URL: http://cve.mitre.org (accessed: 10.04.2023).

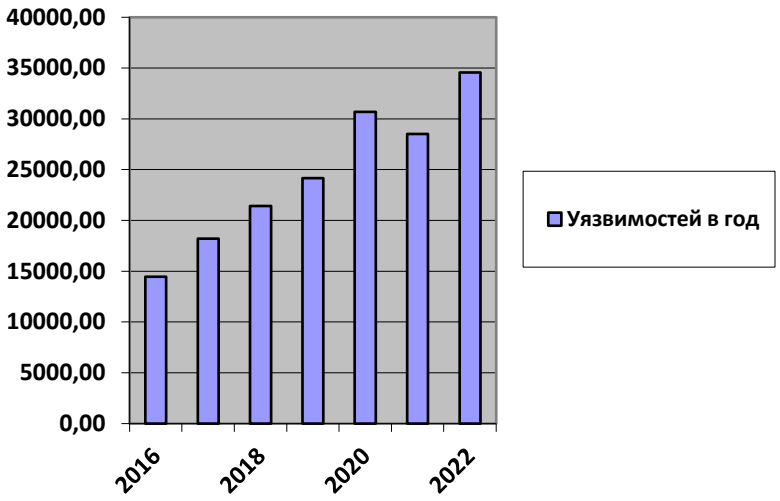

Рис. 3. Диаграмма числа обнаруженных уязвимостей
Fig. 3. Diagram of the number of vulnerabilities detected

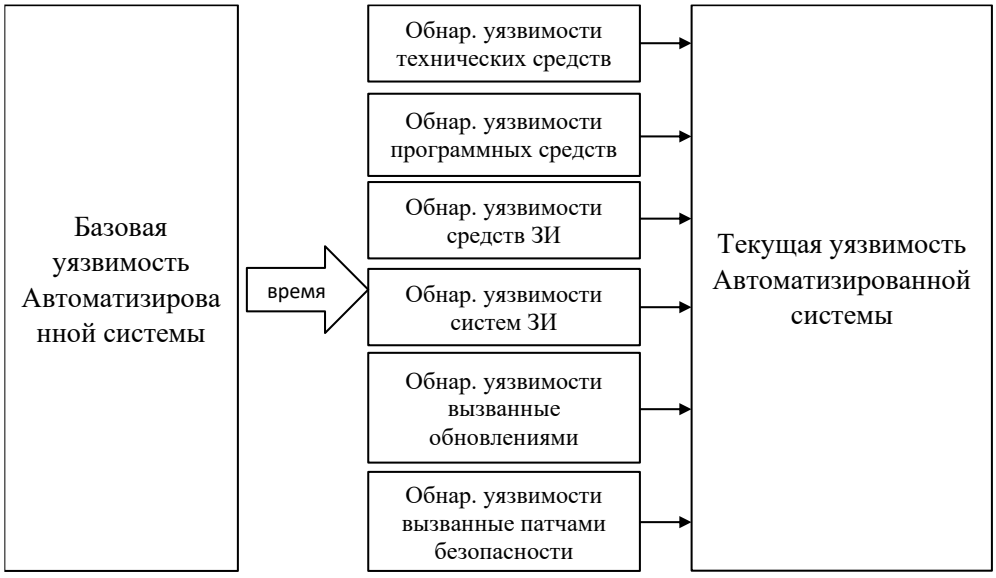

Рис. 4. Схема формирования текущей уязвимости АС
Fig. 4. Diagram of the formation of the current vulnerability of the AS

Интервал, в котором проводится определение уровня текущей уязвимости, предлагается определить как промежуток времени, который дается согласно утвержденной методики ФСТЭК России на устранение уязвимостей. То есть в случае обнаружения уязвимостей уровня критичности «критический» на устранение дается 24 часа, следовательно, следующую проверку текущей уязвимости АС следует проводить через 24 часа после устранения. При отсутствии обнаружения новых уязвимостей, рекомендуется проводить проверку согласно установленным временным рамкам

критичности уязвимостей[7]. Текущая уязвимость АС также должна быть устранена согласно методам, указанным при базовой уязвимости АС. Данная форма сопровождения АС предлагается для использования по всему этапу эксплуатации по всему жизненному циклу АС. Отдельно отмечается, что в случае невозможности устранения уязвимостей в указанные в утвержденной методике сроки, предполагается прекращение обработки защищаемой информации и эксплуатации АС до момента устранения уязвимости. Схема устранения текущей уязвимости АС показана на рис. 5.

Рис. 5. Схема устранения текущей уязвимости АС
Fig. 5. Scheme of elimination of the current vulnerability of the AS

3. Оценка критичности уязвимости

Выше был приведен пример качественной оценки критичности уязвимости, а именно – критическая уязвимость. Всего в методике ФСТЭК России представлено 4 вида критичности уязвимостей, которые характеризуются как качественной, так и количественной оценкой [5]. Соответствие оценок (***V***) ФСТЭК России представлена в табл. 1.

Таблица 1. Соответствие оценок ФСТЭК России

№	Суммарное количество баллов уязвимости	Оценка уровня критичности уязвимости
1.	$7{,}0 \le V \le 10{,}0$	Критичный
2.	$4{,}5 \le V < 7{,}0$	Высокий
3.	$1{,}5 \le V < 4{,}5$	Средний
4.	$V < 1{,}5$	Низкий

Предлагается воспользоваться данной методикой для комплексной оценки. Вышеуказанная методика построена на основе стандарта Common Vulnerability Scoring System разработанного группой экспертов по безопасности National Infrastructure Advisory Council[8]. В этом стандарте определены 5 видов критичности уязвимости (см. табл. 2):

[7]Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств: утв. ФСТЭК России 28 октября 2022 г.: Методический документ ФСТЭК России от 28.02.2022.
[8]Common Vulnerability Scoring System v3.0: Specification Document. FIRST Org. Inc, 2015. – 21 p. URL: https://www.first.org/cvss/specification-document (accessed: 10.04.2023).

Таблица 2. Соответствие оценок стандарта CVSS

№	Количественная оценка	Качественная оценка
1.	$0 \leq V \leq 0.1$	None
2.	$0.1 < V < 4.0$	Low
3.	$4.0 \leq V < 7.0$	Medium
4.	$7.0 \leq V < 9.0$	High
5.	$9.0 \leq V \leq 10.0$	Critical

Так как нулевая оценка соответствует отсутствию возможности достижения уязвимости, либо проведения атаки с каким-либо значительным ущербом, через эту уязвимость, то элементы с данной количественной оценкой можно не учитывать, и пользоваться оценками, приведенными в отечественном методическом документе. Расчет критичности проводится по установленной формуле согласно определенных метрик со своими весовыми коэффициентами:

$$V = I_{cvss} * I_{infr}, \quad (1)$$

где I_{cvss} – показатель, характеризующий уровень опасности уязвимости; I_{infr} – показатель, характеризующий влияние уязвимости программных, программно-аппаратных средств на функционирование информационной системы.

Показатель I_{cvss} определяется путем расчета базовых, временных и контекстных метрик применительно к конкретной информационной системе по методике Common Vulnerability Scoring System (CVSS) 3.0 или 3.1[6] [5]. Отдельно стоит обратить внимание, что в формулах, приведенных разработчиком методики, содержатся числовые коэффициенты, корректирующие показатели формулы. Параметры, применяемые в формулах, приведены в табл. 3.

Стоит отдельно отметить, что стандарт[4] расширяет понятие защищаемых свойств конфиденциальности, целостности, доступности, следующими понятиями: неотказуемость, подотчетность, аутентичность и достоверность, что дополнительно раскрывает важность ряда метрик рассматриваемых методик. В данной работе применяется версия методики CVSS 3.1. В расчете этого показателя применяются следующие метрики[9]:

Параметр **Scope** имеет два значения, не имеющих числовой величины: *Changed* – уязвимость оказывает влияние на другие компоненты системы, *Unchanged* – уязвимость не оказывает влияния на другие компоненты системы.

Вычисление I_{cvss} проводится в следующем порядке:

1) Для базовой (основной) оценки:

В первую очередь проводится оценка влияния уязвимости на конфиденциальность, целостность, доступность (см. табл. 3 «Воздействие на C, I, A»):

$$ISC_{Base} = 1 - \left[\left(1 - Impact_{Conf}\right) * \left(1 - Impact_{Integ}\right) * \left(1 - Impact_{Avail}\right)\right]. \quad (2)$$

[9][b-ITU-T X.1521] Рекомендация МСЭ-Т X.1521 (2016 г.), Система оценки общеизвестных уязвимостей 3.0. URL: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12614&lang=ru (accessed: 10.04.2023).

Таблица 3. Применяемые метрики стандарта CVSS

Показатель	**Значение показателя**	**Числовое значение**
Вектор атаки (Attack Vector)/ уточненный вектор атаки (Modified Attack Vector)	Сетевой (Network)	0,85
	Соседский (Adjacent Network)	0,62
	Локальный (Local)	0,55
	Физический (Physical)	0,2
Сложность атаки (Attack Complexity)/ уточненная сложность атаки (Modified Attack Complexity)	Низкая (Low)	0,77
	Высокая (High)	0,44
Потребность в привилегиях (Privileges Required)/ уточненная потребность в привилегиях (Modified Privileges Required)	Отсутствует (None)	0,85
	Низкая (Low)	0,62 (0,68, если показатель «область действия» (Scope)/ «уточненная область действия» (Modified Scope) имеет значение «меняется» (Changed))
	Высокая (High)	0,27 (0,50, если показатель «область действия» (Scope)/ «уточненная область действия» (Modified Scope) имеет значение «меняется» (Changed))
Взаимодействие с пользователем (User Interaction)/ уточненное взаимодействие с пользователем (Modified User Interaction)	Отсутствует (None)	0,85
	Требуется (Required)	0,62
Воздействие на C, I, A/ уточненное воздействие на C, I, A	Сильное (High)	0,56
	Слабое (Low)	0,22
	Отсутствует (None)	0
Готовность к эксплуатации (Exploit Code Maturity)	Не определено (Not Defined)	1
	Высокая (High)	1
	Функциональная (Functional)	0,97
	Доказана правильность концепции (Proof-of-Concept)	0,94
	Непроверенная (Unproven)	0,91
Уровень устранения (Remediation Level)	Не определено (Not Defined)	1
	Недоступно (Unavailable)	1
	Обходной прием (Workaround)	0,97
	Вре́менное исправление (Temporary Fix)	0,96
	Официальное исправление (Official Fix)	0,95
Достоверность сообщения (Report Confidence)	Не определено (Not Defined)	1
	Подтверждена (Confirmed)	1
	Разумная (Reasonable)	0,96
	Неизвестна (Unknown)	0,92
Важность требований безопасности – важность требований C, I, A (CR)	Не определено (Not Defined)	1
	Высокая (High)	1,5
	Средняя (Medium)	1
	Низкая (Low)	0,5

Затем определяется параметр, в зависимости от воздействия данной уязвимости на другие компоненты системы (ISC):

- Для уязвимости, не оказывающей влияние на другие компоненты системы (*Scope=Unchanged*):

$$ISC = 6.42 * ISC_{Base}. \quad (3)$$

- Для уязвимости, оказывающей влияние на другие компоненты системы (*Scope=Changed*):

$$ISC = 7.52 * (ISC_{Base} - 0.029) - 3.25 * (ISC_{Base} - 0.02)^{15}. \quad (4)$$

Также дополнительно определяется параметр, построенный на основе среды функционирования уязвимости (параметры согласно табл. 3):

$$Exploitability = 8.22 * AttackVector * AttackComplexity * PrivilegeRequired * UserInteraction. \quad (5)$$

Впоследствии чего дается оценка:

Если показатель *ISC* меньше или равен нулю, то показатель характеризующий уровень опасности уязвимости равен нулю:

$$I_{cvss} = 0. \quad (6)$$

В ином случае, показатель определяется по формуле, которая выбирается в зависимости от влияния на другие компоненты системы:

- Для уязвимости, не оказывающей влияние на другие компоненты системы (*Scope=Unchanged*):

$$I_{cvss} = Roundup(Minimum[(ICS + Exploitability), 10]). \quad (7)$$

- Для уязвимости, оказывающей влияние на другие компоненты системы (*Scope=Changed*):

$$I_{cvss} = Roundup(Minimum[1.08 * (ISC + Exploitability), 10]), \quad (8)$$

где $Roundup$ – функция, округляющая значение, заданное с точностью до одного знака после запятой, большее или равное входному значению[7], $Minimum$ – функция возвращает минимальное значение из нескольких операндов.

Например, *Roundup*(4.02) = 4.1, а *Roundup*(4.00) = 4.0.

Для удобства обозначения результат, полученный при основном вычислении, далее будет обозначаться как I_{cvss1} в целях недопущения смешения обозначений в формулах.

2) Для дополнительной (уточненной) оценки по характеристикам, изменяемым со временем:

В данном дополнительном вычислении, проводится учёт зрелости уязвимости с точки зрения досягаемости её злоумышленником (факта её достижения), доступности средств устранения, и достоверности наличия уязвимости (параметры указаны в табл. 3):

$$I_{cvss} = Roudup(I_{cvss1} * ExploitCodeMaturity * RemediationLevel * * ReportConfidence). \quad (9)$$

3) Для дополнительной (уточненной) оценки в зависимости от среды функционирования и корректирующих оценок:

В данном вычислении, дополнительно учитываются корректирующие оценки среды функционирования, а также требования к конфиденциальности целостности доступности (параметры указаны в табл. 3).

В первую очередь, так же, как и при базовом вычислении, определяются требования к конфиденциальности, целостности, доступности, но в совокупности с уровнем требований к конфиденциальности, целостности, доступности:

$$ISC_{Modified} = Minimum\left(\left[\begin{matrix}1-(M.ICon f*CR)*(1-M.IInteg*IR)*\\ *(1-M.IAvail*AR)\end{matrix}\right], 0.915\right). \quad (10)$$

Также дополнительно определяется параметр, построенный на основе среды функционирования уязвимости (параметры согласно табл. 3):

$$M.Exploitability = 8.22 * M.AttackVector * M.AttackComplexity * \\ * M.PrivilegeRequired * M.UserInteraction. \quad (11)$$

Затем на подобии базовой оценки, определяется величина, связанная с корректирующим параметром воздействия уязвимости на другие элементы системы (*M.ISC*):

- Для уязвимости, не оказывающей влияние на другие компоненты системы (M.*Scope=Unchanged*):

$$M.ISC = 6.42 * ISC_{Modified.} \quad (12)$$

- Для уязвимости, оказывающей влияние на другие компоненты системы (*M.Scope=Changed*):

$$M.ISC = 7.52 * \left(ISC_{Modified} - 0.029\right) - 3.25 * (ISC_{Modified} * 0.9731 - 0.02)^{13}. \quad (13)$$

После чего уточненная оценка определяется следующим образом:

Если показатель *M.ISC* меньше или равен нулю, то показатель характеризующий уровень опасности уязвимости равен нулю:

$$I_{cvss} = 0. \quad (14)$$

- Для уязвимости, не оказывающей влияние на другие компоненты системы (M.*Scope=Unchanged*):

$$I_{cvss} = Roundup\left(\begin{matrix}Roundup[Minimum([M.Impact + M.Exploitability], 10] *\\ * ExploitCodeMaturity * RemediationLevel * ReportConfidence\end{matrix}\right). \quad (15)$$

- Для уязвимости, оказывающей влияние на другие компоненты системы (*M.Scope=Changed*):

$$I_{cvss} = Roundup\left(\begin{matrix}Roundup[Minimum(1.08 * [M.Impact + M.Exploitability], 10] *\\ * ExploitCodeMaturity * RemediationLevel * ReportConfidence\end{matrix}\right). \quad (16)$$

Показатель I_{infr} определяется согласно утвержденной методики по следующей формуле:

$$I_{infr} = (k * K) + (l * L) + (p * P), \quad (17)$$

где K – показатель, характеризующий тип компонента информационной системы, подверженного уязвимости;

L – показатель, характеризующий количество уязвимых компонентов информационной системы (автоматизированных рабочих мест (АРМ), серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов);

P – показатель, характеризующий влияние уязвимого компонента на защищенность периметра информационной системы;

k, l, p – весовые коэффициенты показателей.

Расчет весовых коэффициентов и оценок показателей, определяющих влияние уязвимости программных, программно-аппаратных средств на информационную систему, проводится в соответствии с табл. 4.

Таблица 4. Расчет весовых коэффициентов и оценок показателей

№ п/п	Показатель	Вес	Значение	Оценка	Итог
1	Тип компонента информационной системы, подверженного уязвимости (К)	0,4	Уязвимости подвержены компоненты информационной системы, обеспечивающие реализацию критических процессов (бизнес-процессов), функций, полномочий	1	0,4
			Уязвимости подвержены серверы	0,8	0,32
			Уязвимости подвержено телекоммуникационное оборудование, система управления сетью передачи данных	0,8	0,32
			Уязвимости подвержены АРМ	0,5	0,20
			Уязвимости подвержены другие компоненты	0,5	0,20
2	Количество уязвимых компонентов информационной системы (АРМ, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов) (L)	0,2	Более 70% компонентов от общего числа компонентов в информационной системе	1	0,2
			50–70% компонентов от общего числа компонентов в информационной системе	0,8	0,16
			10–50% компонентов от общего числа компонентов в информационной системе	0,6	0,12
			Менее 10% компонентов от общего числа компонентов в информационной системе	0,5	0,10
3	Влияние на эффективность защиты периметра системы, сети (Р)	0,4	Уязвимое программное, программно-аппаратное средство доступно из сети «Интернет»	1	0,4
			Уязвимое программное, программно-аппаратное средство недоступно из сети «Интернет»	0,5	0,2

По окончанию вычисления, показатель критичности V вычисляется по формуле (1), определяет критичность той или иной уязвимости.

4. Оценка защищенности АС на основе совокупности уязвимостей

В целях достижения комплексной оценки защищенности, предлагается сведение массива показателей критичности в матрицу, где столбцом определяется элемент АС подверженный уязвимости, а строкой критичность уязвимости данного элемента.

$$A_{\text{текущая/базовая}} = \begin{bmatrix} V_{1,1} & V_{1,2} & \dots & V_{1,j} \\ V_{2,1} & V_{2,2} & \dots & V_{2,j} \\ \dots & \dots & \dots & \dots \\ V_{i,1} & V_{i,2} & \dots & V_{i,j} \end{bmatrix}, \quad (18)$$

где $V_{i,j}$ – показатель, критичности уязвимости элемента АС; i – порядковый номер уязвимости элемента АС; j – порядковый номер элемента АС.

Данной формой записи и предлагается записывать базовую и текущую уязвимость АС. При этом определение элемента с максимальным значением в столбце n, будет указывать на критичность уязвимости n-го элемента АС:

$$V_{n.\text{крит.}} = \max(A_{i,n}), \quad (19)$$

где i – порядковый номер максимально критичной уязвимости элемента АС; n – порядковый номер элемента АС.

Элемент Аij с наибольшим значением в матрице будет указывать на уязвимость всей АС в количественной величине, которая может быть переведена в качественную согласно табл. 1.

$$V_{\text{крит.}} = \max(A_{i,j}), \quad (20)$$

где i – порядковый номер максимально критичной уязвимости элемента АС; j – порядковый номер максимально критичного элемента АС.

В связи с тем, что рассчитываемый показатель количественной оценки критичности уязвимости нормирован, то предлагается следующая формула оценки защищенности АС, определяющая вероятность неиспользования данной уязвимости злоумышленником (чем выше критичность уязвимости, тем выше вероятность её использования злоумышленником):

$$P_{\text{н.}} = \left(1 - \frac{V_{\text{крит.}}}{10}\right), \quad (21)$$

где $V_{\text{крит.}}$ наибольший показатель критичности, из всех элементов АС.

Значения данной величины, будут отражать уровень защищенности АС в зависимости от уязвимости компонент. Для перевода количественной оценки в качественную может применяться таблица (см. табл. 5) значений аналогичная таблице, утвержденной ФСТЭК России:

Таблица 5. Соответствие оценок защищенности

№	Количественная оценка	Оценка уровня защищенности
1.	$0{,}7 \le P_{н.} \le 1{,}0$	Высокий
2.	$0{,}45 \le P_{н.} < 0{,}7$	Выше среднего
3.	$0{,}15 \le P_{н.} < 0{,}45$	Средний
4.	$P_{н.} < 0{,}15$	Низкий

В зависимости от оценки текущего уровня защищенности предлагается применение временного показателя $T_{убф}$ (который возможно использовать для моделирования процессов), обозначающего условно безопасный период функционирования АС которой присвоен уровень защищенности:

- «Низкий», $T_{убф}$ = 24 часа;
- «Средний», $T_{убф}$ = 168 часов;
- «Выше среднего», $T_{убф}$ = 672 часа;

– «Высокий», $T_{убф}$ = 2900 часов.

При невозможности устранения наиболее критичной уязвимости в установленный выше промежуток времени, предполагается завершение эксплуатации данной АС, до момента устранения этой уязвимости. Примечание: при обнаружении более критической, либо равно критической уязвимости, уже существующей ранее обнаруженной не устранённой уязвимости, показатель $T_{убф,}$ либо не изменяется (в случае равенства критичности старой и новой уязвимости, период времени отсчета сохраняется от старой уязвимости), либо уменьшается согласно приведенным временным показателям до величины соответствующего уровня защищенности (критичности уязвимости). Считается целесообразным проведение дальнейшего исследования, в целях построения модели оценки уровня защищенности АС, на основе уязвимости. А также, в связи с неопределенностью всех факторов, влияющих на рост числа выявляемых уязвимостей, считается целесообразным исследование путем построения модели на основе теории серых систем для прогнозирования числа обнаруженных в будущем уязвимостей [15–17].

Заключение

В данной работе представлены концептуальные основы оценки уровня защищенности АС на основе их уязвимости, а именно:

– проведен анализ, регламентирующих стандартов и методических рекомендаций, связанных с уязвимостью информационных систем;

– проведен анализ формирования совокупностей уязвимостей, предложено определение базовой уязвимости АС и текущей уязвимости АС, а также путей их устранения;

– проведена адаптация и описание процесса оценки критичности уязвимости стандарта CVSS 3.1;

– предложена методика оценки уровня защищенности, путем анализа критичности уязвимости АС;

– сделаны выводы о направлении дальнейшего исследования.

СПИСОК ЛИТЕРАТУРЫ:

1. Ланкин О.В. Системно-комплексный кибернетический подход к формированию методологических основ интеллектуальной защиты информации от несанкционированного доступа. О.В. Ланкин, В.И. Сумин, Е.В. Воронова. Вестник Воронежского государственного технического университета. 2011, т. 7, № 8, с. 174–176. – EDN: NYIJQT.
2. Бокова О.И., Дровникова И.Г., Етеппев А.С., Рогозин Е.А., Хвостов В.А. (2019). Методики оценивания надежности систем защиты информации от несанкционированного доступа в автоматизированных системах. Труды СПИИРАН, 18(6), с. 1301–1332. DOI: http://dx.doi.org/10.15622/sp.2019.18.6.1301-1332. – EDN: YBHXOB.
3. Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа. Пособие. Воронеж: Кварта, 2015. – 440 с.
4. Дровникова И.Г., Етепнев А.С., Рогозин Е.А. Основные виды уязвимостей и взаимосвязь компонентов безопасности при обосновании показателей надёжности системы защиты информации от несанкционированного доступа в автоматизированных системах. Приборы и системы. Управление, контроль, диагностика. 2019, № 3, с. 59–64. DOI: http://dx.doi.org/10.25791/pribor.03.2019.508.
5. Дойникова Е.В. Чечулин А.А., Котенко И.В. Оценка защищенности компьютерных сетей на основе метрик CVSS. Информационно-управляющие системы. 2017, № 6(91), с. 76–87. DOI: http://dx.doi.org/10.15217/issn1684-8853.2017.6.76. – EDN: ZXWUWH.
6. Кубарев А.В. Подход к формализации уязвимостей информационных систем на основе их классификационных признаков. Вопросы кибербезопасности. 2013, № 2(2), с. 29–33. – EDN: SZEDHH.
7. Коноваленко С.А., Королев И.Д. Выявление уязвимостей информационных систем посредством комбинированного метода анализа параметрических данных, определяемых системами мониторинга

вычислительных сетей. Альманах современной науки и образования. 2016, № 11(113), с. 60–66. – EDN: XEEDXH.
8. Сердечный А.Л., Тарелкин М.А., Ломов А.А., Симонов К.В. Карты источников, содержащих сведения об уязвимостях программного обеспечения. Информация и безопасность. 2019, т. 22, № 3, с. 411–422. – EDN: ZOUMGN.
9. Федорченк А.В., Чечулин А.А., Котенко И.В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей. Информационно-управляющие системы. 2014, № 5(72), с. 72–79. – EDN: SXXXKH.
10. Сердечный А.Л.,. Герасимов И.В., Макаров О.Ю. и др. Технология выявления сведений об уязвимостях сторонних компонентов программного обеспечения с открытым исходным кодом. Информация и безопасность. 2020, т. 23, № 3, с. 347–364. DOI: http://dx.doi.org/10.36622/VSTU.2020.23.3.003. – EDN: PYXOUT.
11. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения. Вопросы кибербезопасности. 2014, № 3(4), с. 20–28. – EDN: SSYPXV.
12. Russell R. et al. Automated Vulnerability Detection in Source Code Using Deep Representation Learning. 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA. 2018, p. 757–762. DOI: http://dx.doi.org/10.1109/ICMLA.2018.00120.
13. Wang T., Wei T., Gu G. and Zou W. TaintScope: A Checksum-Aware Directed Fuzzing Tool for Automatic Software Vulnerability Detection. IEEE Symposium on Security and Privacy, Oakland, CA, USA. 2010, p. 497–512. DOI: http://dx.doi.org/10.1109/SP.2010.37.
14. 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: http://dx.doi.org/10.1109/JPROC.2020.2993293.
15. Ван Ю. Прогнозирование объемов перевозок пассажиров на основе теории "серых систем". Вестник Белорусского государственного университета транспорта: наука и транспорт. 2021, № 1(42), с. 77–81. – EDN: OKGSXG.
16. Deng J.L. Introduction to Grey system theory. Journal of Grey System 1 (1989): 1-24. URL: https://www.semanticscholar.org/paper/Introduction-to-Grey-system-theory-Deng/a6d38c2f78a12b92464ef95b89d0567e01262631 (дата обращения: 10.04.2023).
17. Bindhu B.K. & Madhu G. (2017) Application of grey system theory on the influencing parameters of aerobic granulation in SBR, Environmental Technology, 38:17, p. 2143–2152. DOI: http://dx.doi.org/10.1080/09593330.2016.1246617.

REFERENCES:

[1] Lankin O.V., Sumin V.I., Voronova E.V. System-integrated cybernetic approach to the formation of methodological foundations of intellectual protection of information from unauthorized access, Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2011, vol. 7, no. 8, p. 174–176 (in Russian). – EDN: NYIJQT.
[2] Bokova O., Drovnikova I., Etepnev A., Rogozin E., Khvostov V. (2019). Methods of Estimating Reliability of Information Security Systems which Protect from Unauthorized Access in Automated Systems. SPIIRAS Proceedings, 18(6), p. 1301–1332. DOI: http://dx.doi.org/10.15622/sp.2019.18.6.1301-1332 (in Russian). – EDN: YBHXOB.
[3] Yazov Yu.K., Solov'ev S.V. Zashchita informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa. Posobie. Voronezh: Kvarta, 2015. 440 p. (in Russian).
[4] Drovnikova I.G., Etepnev A.S., Rogozin E.A. The main types of vulnerabilities and the relationship of security components in substantiating the reliability indicators of the information protection system from unauthorized access in automated systems. Pribory i sistemy. Upravlenie, kontrol', diagnostika. 2019, no. 3, p.59–64. DOI: http://dx.doi.org/10.25791/pribor.03.2019.508 (in Russian).
[5] Dojnikova E.V., CHechulin A.A., Kotenko I.V. Assessment of the security of computer networks based on CVSS metrics. Informacionno-upravlyayushchie sistemy. 2017, no. 6(91), p. 76–87. DOI: http://dx.doi.org/10.15217/issn1684-8853.2017.6.76 (in Russian). – EDN: ZXWUWH.
[6] Kubarev A.V. Approach to formalization of vulnerabilities of information systems based on their classification features. Voprosy kiberbezopasnosti. 2013, no. 2(2), p. 29–33 (in Russian). – EDN: SZEDHH.
[7] Konovalenko S.A., Korolev I.D. Identification of vulnerabilities of information systems by means of a combined method of analysis of parametric data determined by monitoring systems of computer networks, Al'manah sovremennoj nauki i obrazovaniya. 2016, no. 11(113), p. 60–66 (in Russian) – EDN: XEEDXH.

[8] Serdechnyj A.L., Tarelkin M.A., Lomov A.A., Simonov K.V. Maps of sources containing information about software vulnerabilities. Informaciya i bezopasnost'. 2019, vol. 22, no. 3, p. 411–422 (in Russian). – EDN: ZOUMGN.
[9] Fedorchenko A.V., CHechulin A.A., Kotenko I.V. Research of open databases of vulnerabilities and assessment of the possibility of their application in systems of security analysis of computer networks. Informacionno-upravlyayushchie sistemy. 2014, no. 5(72), p. 72–79 (in Russian). – EDN: SXXXKH.
[10] Serdechnyj A.L., Gerasimov I.V., Makarov O.YU. i dr. Technology for identifying information about vulnerabilities of third-party components of open source software. Informaciya i bezopasnost'. 2020, vol. 23, no. 3, p.347–364 (in Russian). – EDN: PYXOUT.
[11] Avetisyan A.I., Belevancev A.A., Chuklyaev I.I. Technologies of static and dynamic analysis of software vulnerabilities. Voprosy kiberbezopasnosti. 2014, no. 3(4), p. 20–28 (in Russian). – EDN: SSYPXV.
[12] Russell R. et al. Automated Vulnerability Detection in Source Code Using Deep Representation Learning. 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA. 2018, p. 757–762. DOI: http://dx.doi.org/10.1109/ICMLA.2018.00120.
[13] Wang T., Wei T., Gu G. and Zou W. TaintScope: A Checksum-Aware Directed Fuzzing Tool for Automatic Software Vulnerability Detection. IEEE Symposium on Security and Privacy, Oakland, CA, USA. 2010, p. 497–512. DOI: http://dx.doi.org/10.1109/SP.2010.37.
[14] 17. 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: http://dx.doi.org/10.1109/JPROC.2020.2993293.
[15] Yu. Van. Forecasting passenger traffic volumes based on the theory of "gray systems" Vestnik Belorusskogo gosudarstvennogo universiteta transporta: nauka i transport. 2021, no. 1(42), p. 77–81 (in Russian). – EDN: OKGSXG.
[16] Deng J.L. Introduction to Grey system theory. Journal of Grey System 1 (1989): 1-24. URL: https://www.semanticscholar.org/paper/Introduction-to-Grey-system-theory-Deng/a6d38c2f78a12b92464ef95b89d0567e01262631 (accessed: 14.04.2023).
[17] Bindhu B.K. & Madhu G. (2017) Application of grey system theory on the influencing parameters of aerobic granulation in SBR, Environmental Technology, 38:17, p. 2143–2152. DOI: http://dx.doi.org/10.1080/09593330.2016.1246617.

Поступила в редакцию – 28 февраля 2023 г. Окончательный вариант – 19 апреля 2023 г.
Received – February 28, 2023. The final version – April 19, 2023.