Управление рисками и безопасностью

Подход к автоматизации оценки уровня критичности уязвимостей с использованием машинного обучения

А.Ю. Тихонов

Российский государственный университет нефти и газа (НИУ) им. И.М. Губкина», г. Москва, Россия

Аннотация. В статье отражены результаты исследования вопроса повышения эффективности деятельности специалистов по защите информации при проведении оценки уровня критичности уязвимостей программных и программно-аппаратных средств. Обозначена важность данной деятельности для комплексного обеспечения безопасности информационных систем. Представлены результаты обзора существующих решений в области повышения ее эффективности путем автоматизации. Предложен подход к автоматизации оценки уровня критичности уязвимостей с использованием машинного обучения, представлено его описание, преимущества и план практической реализации. Обозначены перспективные направления развития предложенного подхода.

Ключевые слова: *искусственный интеллект, машинное обучение, уязвимость, уровень критичности, информационная система, информационная безопасность.*

DOI: 10.14357/20790279260314 **EDN:** QPQHJI

Введение

Оценка уровня критичности уязвимостей программных и программно-аппаратных средств необходима по ряду причин, связанных с ростом количества киберугроз, требованиями регуляторов, необходимостью управления рисками и обеспечением непрерывности функционирования информационных систем, в том числе на объектах критической информационной инфраструктуры (далее – КИИ). Перечислим и кратко охарактеризуем основные из них.

1. Рост киберугроз и их эволюция. Злоумышленники постоянно ищут слабые места в информационных системах, и даже уязвимость, имеющая в общем случае низкий уровень опасности, может привести к серьезному нарушению безопасности конкретной информационной системы. Помимо обнаружения неизвестных ранее уязвимостей в старых программных и программно-аппаратных средствах, новые появляются в информационных системах по мере установки в них нового программного обеспечения и оборудования. Оценка критичности уязвимостей позволяет оперативно выявлять и устранять наиболее опасные уязвимости до того, как ими воспользуются злоумышленники.

Согласно [1] классификация уязвимостей является одним из факторов, непосредственно влияющих на возможность исключения несанкционированного доступа к информационной системе.

2. Соблюдение нормативных требований. В Российской Федерации действуют достаточно строгие

требования к оценке и управлению уязвимостями. Так, методика ФСТЭК России от 30 июня 2025 года определяет порядок оценки уровня критичности уязвимостей в программных и программно-аппаратных средствах [2]. При этом в обновленной редакции она распространяется и на государственные информационные системы, значимые объекты КИИ, а также на государственные унитарные предприятия и госучреждения [3]. Несоблюдение требований может привести к наложению штрафных санкций, юридическим проблемам и потере доверия со стороны партнеров.

3. Приоритезация в расходовании ресурсов и эффективное управление рисками. Оценка критичности позволяет сосредоточить усилия и ресурсы на устранении наиболее опасных уязвимостей в первую очередь, что повышает эффективность работы подразделений информационной безопасности. Это особенно важно в условиях ограниченных кадровых и финансовых ресурсов.

4. Защита конфиденциальных данных и бизнес-операций. Эксплуатация уязвимости может привести к утечке конфиденциальных данных (информации клиентов, финансовых сведений, интеллектуальной собственности), что влечет финансовые потери и репутационный ущерб. Оценка критичности помогает выявить слабые места в защите, которые могут стать точками входа для злоумышленников, и своевременно их устранить.

5. Обеспечение непрерывности функционирования информационных систем. Уязвимости могут нарушить работу критически важных сервисов и процессов. Например, сбой в работе серверов или сетевых устройств может остановить производственные линии, финансовые операции или другие бизнес-процессы. Оценка уровня критичности позволяет минимизировать риски простоев и сохранить работоспособность системы.

6. Необходимость регулярного пересмотра и адаптации. Статус уязвимостей может меняться со временем: появляются новые эксплойты, выходят обновления для уязвимых компонент системы, изменяются условия эксплуатации. Указанная методика ФСТЭК России требует регулярной переоценки уровня критичности уязвимостей, в том числе при появлении новых сведений об уязвимости (например, при выпуске обновлений безопасности или при появлении средств эксплуатации уязвимости в открытом доступе). Это подчеркивает важность постоянного мониторинга и актуализации оценок уровня критичности уязвимостей.

7. Интеграция в процессы разработки и эксплуатации. В современных подходах, таких как DevSecOps, оценка уязвимостей встраивается в жизненный цикл разработки ПО [4]. Это позволяет выявлять и устранять потенциальные проблемы на ранних этапах, снижая затраты на исправление ошибок в будущем.

8. Улучшение реагирования на инциденты. Четкое понимание уровня критичности уязвимостей помогает быстрее и эффективнее реагировать на кибератаки. Оператор информационной системы может заранее усилить защиту в уязвимых местах, что снижает время на устранение последствий инцидентов.

Таким образом, оценка уровня критичности уязвимостей является одним из ключевых элементов системы информационной безопасности, который способствует эффективному использованию имеющихся ресурсов, минимизации рисков информационной безопасности и обеспечению надежной ее защиты в условиях постоянно меняющихся угроз.

В данной статье предложен подход к автоматизации оценки уровня критичности уязвимостей программных, программно-аппаратных средств с использованием машинного обучения для учета значений, рассчитанных ранее экспертным методом по соответствующей методике ФСТЭК России для данной конкретной информационной системы.

1. Существующий подход к оценке уровня критичности уязвимостей программных и программно-аппаратных средств

В настоящее время в Российской Федерации для принятия обоснованного решения о необходимости и приоритетности устранения уязвимостей, выявленных в программных и программно-аппаратных средствах, применяется разработанная ФСТЭК России методика оценки уровня критичности уязвимостей программных и программно-аппаратных средств от 30 июня 2025 г. (далее – Методика).

Методика обязательна к применению операторами государственных информационных систем, государственных органов, предприятий и учреждений, а также операторами значимых объектов КИИ Российской Федерации.

При определении критичности уязвимостей в соответствии с Методикой учитываются базовый уровень опасности уязвимости, рассчитанный в соответствии со стандартом расчета количественных оценок уязвимости (Common Vulnerability Scoring System, CVSS), влияние уязвимости на функционирование данной информационной системы, возможность эксплуатации оцениваемой

уязвимости в ней, а также возможные последствия от эксплуатации уязвимости для данной информационной системы.

Несмотря на то, что актуальная редакция Методики достаточно хорошо проработана и адаптирована к российским реалиям, ее применение на практике связано с рядом сложностей. Так, она предполагает, что оценка уровня критичности уязвимостей программных и программно-аппаратных средств проводится подразделением (специалистами) по защите информации (информационной безопасности) (далее – Эксперты) оператора информационной системы.

При определении критичности Методикой предписано получать исходные данные об уязвимостях их базы, содержащейся в Банке данных угроз безопасности информации ФСТЭК России, с официальных информационных ресурсов разработчиков программного обеспечения и программно-аппаратных средств и исследователей в области информационной безопасности, а также из иных источников, содержащих сведения об известных уязвимостях. При этом указанная информация имеет существенный объем. Одна только база данных уязвимостей ФСТЭК России в настоящее время содержит информацию о порядка 82 тыс. уязвимостей. При этом в отношении рассматриваемых уязвимостей эксперты должны осуществить математические расчеты показателей по представленной в Методике формуле.

Также Методика обязует экспертов пересчитывать уровень критичности уязвимостей при появлении новых сведений о них.

Таким образом оценка уровня критичности и постоянная его актуализация для уязвимостей, содержащихся в программных и программно-аппаратных средствах крупных информационных систем может привести к значительной постоянной нагрузке на специалистов по информационной безопасности. А в условиях существующего кадрового дефицита квалифицированных специалистов, особенно в организациях государственного сектора, указанная работа может оказаться крайне затруднительной.

Кроме того, частные показатели I_{infr}, I_{at} и I_{imp}[1], используемые при оценке уровня критичности уязвимостей в соответствии с рассматриваемой Методикой, имеют относительно субъективный характер и могут интерпретироваться разными экспертами по-разному.

2. Повышение эффективности существующего подхода к оценке уровня критичности уязвимостей

Необходимость принятия операторами информационных систем обоснованного и своевременного решения о приоритетности устранения уязвимостей, выявленных в программных и программно-аппаратных средствах, определяет актуальность работы по повышению эффективности деятельности экспертов по оценке уровня критичности уязвимостей программных, программно-аппаратных средств.

При этом необходимо отметить, что в настоящее время имеет место всплеск использования злоумышленниками технологий искусственного интеллекта при осуществлении компьютерных атак, что подтверждается все возрастающим количеством публикаций на эту тему. Так в [5] приводятся данные об активном использовании больших языковых моделей (Large Language Model, LLM) для генерации и обфускации вредоносного программного кода, создания текста фишинговых электронных писем, сообщений, подготовленных с использованием методов социальной инженерии, подбора паролей, разгадывания CAPTCHA. Кроме того, согласно [6] ключевым сдвигом 2025 года стало кардинальное увеличение скорости атак – теперь время между обнаружением уязвимости и ее эксплуатацией сократилось с недель до дней и часов. В итоге традиционные процессы реагирования на компьютерные инциденты больше не успевают за реальностью.

В контексте изложенного задача повышения эффективности деятельности экспертов по оценке уровня критичности уязвимостей программных и программно-аппаратных средств становится особенно актуальной. Одним из возможных путей повышения эффективности указанной деятельности является внедрение средств автоматизированной оценки уровня критичности уязвимостей программных, программно-аппаратных средств, что позволит преодолеть указанные выше сложности практического применения Методики.

В результате обзора имеющихся публикаций по тематике автоматизации оценки уровня критичности уязвимостей, учитывающих требования Методики, выявлено несколько вариантов, которые условно можно разделить на две основные группы: готовые коммерческие продукты для сканирования уязвимостей и решения на базе платформ SGRC.

[1] I_{infr} – показатель, характеризующий влияние уязвимости программных, программно-аппаратных средств на функционирование информационных систем;

I_{at} – показатель, характеризующий возможность эксплуатации уязвимости программных, программноаппаратных средств в информационных системах;

I_{imp} – показатель, характеризующий последствия эксплуатации уязвимости программных, программноаппаратных средств в информационных системах.

Ряд российских разработчиков программного обеспечения для сканирования уязвимостей добавили функции по частичной автоматизации оценки уровня критичности уязвимостей в соответствии с Методикой в свои программные продукты [7]. Среди отечественных решений данной группы наибольшего внимания заслуживают:

- продукт RedCheck от компании Алтэкс-Софт, сертифицированный ФСТЭК и включенный в реестр российского программного обеспечения;
- бесплатный продукт ScanOVAL, также разработанный Алтэкс-Софт, и ориентированный на проверку соответствия информационных систем требованиям ФСТЭК России;
- продукт «Сканер-ВС 6», обеспечивающий комплексную оценку защищенности в соответствии с методиками ФСТЭК России;
- Solar appScreener – российский статический анализатор кода приложений на наличие уязвимостей и определения уровня их опасности [8].

Все указанные продукты поддерживают интеграцию с Банком данных угроз безопасности информации ФСТЭК России и выводят информацию об уровне опасности найденных уязвимостей, рассчитанном в соответствии с CVSS, но не вычисляют итоговый уровень их критичности по формуле, представленной в Методике. Программный продукт «Сканер-ВС 6» в редакции Enterprise предоставляет пользователям возможность регистрировать свои уязвимости при помощи конструктора, в том числе задавая им уровень критичности, который должен быть предварительно получен (рассчитан) пользователем самостоятельно.

Программные решения для автоматизации управления информационной безопасностью, рисками и соответствием нормативным требованиям (Security Governance, Risk and Compliance, SGRC) позволяют автоматизировать не только оценку уровня критичности уязвимостей, но и весь процесс управления ими, включая интеграцию с различными источниками данных. В данном случае автоматизация может строить по следующей схеме: сканер уязвимостей (например, ScanOVAL или RedCheck) собирает данные об уязвимостях и версиях ПО в информационной системе, передает их в систему SGRC, которая уже применяет логику Методики ФСТЭК России при оценке уровня критичности уязвимостей и формирует отчеты для принятия решений [9].

Среди отечественных решений данной группы можно привести такие программные платформы как «КиберОснова SGRC» и SECURITM.

Указанные SGRC-системы представляют собой многофункциональные комплексные средства автоматизации управления информационной безопасностью, в которых приоритезация уязвимостей является одной из множества опций. При этом они не предоставляют возможности автоматической оценки уровня критичности обнаруженных уязвимостей, а предполагают повышение удобства работы специалиста по оценке уровня критичности уязвимостей путем частичной автоматизации его деятельности. Кроме того, в результате рассмотрения документации на указанные системы не было обнаружено упоминания того, что оценка уровня критичности уязвимостей осуществляются с учетом накопленного предыдущего опыта экспертов по работе с данной конкретной информационной системой.

На основании результатов проведенного анализа представляется целесообразным автоматизировать работу эксперта по оценке уровня критичности уязвимостей программных, программно-аппаратных средств при помощи специализированного легковесного инструмента, учитывая при этом предыдущий опыт оценки уязвимостей в данной конкретной информационной системе.

3. Подход к автоматизации оценки уровня критичности уязвимостей программных и программно-аппаратных средств с использованием машинного обучения

Из приведенных в [10] определений следует, что машинное обучение (Machine Learning, ML) представляет собой область искусственного интеллекта, в которой компьютерные системы самостоятельно учатся находить закономерности в данных на основании накопленного опыта, не будучи явно запрограммированными на выполнение конкретных правил. При этом ключевыми преимуществами машинного обучения являются: отсутствие явного программирования алгоритма работы, повышение качества результатов с ростом объема исходных данных, предоставление возможности автоматизации сложных задач (распознавание, прогнозирование, классификация), активное применение в кибербезопасности для быстрой и объективной оценки рисков. Таким образом можно рассматривать машинное обучение в качестве рационального варианта решения задачи автоматизации работы эксперта по оценке уровня критичности.

Одни из основных типов задач, которые эффективно решаются при помощи машинного обучения – это кластеризация и классификация. Пред-

лагаемые далее разбиение множества уязвимостей на классы сходных между собой и оценка уровня критичности уязвимостей будут являться задачами кластеризации и классификации, соответственно. Ключевые методы обучения при этом – с учителем и без него [11].

Анализ существующих публикаций показал, что имеется ряд практически реализованных подходов к автоматизации работы экспертов с информацией об уязвимостях на основе машинного обучения.

Так, в [12] авторы описывают созданную ими трансформерную модель на базе модели RoBERTa, дообученную на более чем 600 000 реальных уязвимостей. Полученная модель способна предсказывать уровень опасности уязвимостей (CVSS Score) напрямую по текстовому ее описанию, еще до появления официальной CVSS-оценки, что позволяет аналитикам получать оперативную оценку в течение нескольких секунд вместо дней ручного анализа.

Российские исследователи предложили гибридный подход, совмещающий NLP-методы (BERT) и классическое машинное обучение (Random Forest) для прогнозирования CVSS Score на основе текстовых описаний уязвимостей (Common Vulnerabilities and Exposures, CVE) из национальной базы данных уязвимостей США (National Vulnerability Database, NVD) [13].

Другими исследователями специально для описаний уязвимостей из банка данных угроз безопасности информации (далее – БДУ) ФСТЭК России была обучена модель на базе ruRoberta-large. Она классифицирует русскоязычные описания уязвимостей по уровням критичности (низкий, средний, высокий, критический) [14].

Некоторые исследователи провели эксперименты по применению для классификации ошибок в программном и аппаратном обеспечении (Common Weakness Enumeration, CWE), прогнозирования CVSS Score и уровня критичности уязвимостей больших языковых моделей (LLM). [15,16] В одном случае в качестве исходных данных использовалась информация об уязвимостях из NVD, в другом – специализированный набор данных для анализа безопасности BinPool. В целом оба эксперимента продемонстрировали хорошие результаты для решения указанных задач, но в обоих случаях наблюдалось устойчивое смещение результатов в сторону средних значений уровня критичности уязвимостей.

Среди рассмотренных реализаций наибольший интерес вызывает фреймворк FRAPE (Risk Assessment, Prioritization and Explainability) [17]. При его создании разработчики использовали комбинацию активного обучения (Active Learning) и обучения с учителем для создания ML-модели, которая способна накапливать опыт экспертов по безопасности. В качестве исходных данных использовалась информация об уязвимостях из NVD. Наилучшие результаты разработанная система показала для выявления уязвимостей критического уровня, при этом качество полученных результатов оказалось сопоставимым с работе экспертов-аналитиков.

Предлагаемый подход к автоматизации оценки уровня критичности уязвимостей программных и программно-аппаратных средств с использованием машинного обучения является развитием изложенных выше наработок с целью:

- предсказания уровня критичности уязвимостей (а не только их CVSS Score);
- учета опыта экспертов по работе с конкретной информационной системой;
- адаптации к применению в условиях действия российского законодательства (описание уязвимостей из БДУ ФСТЭК России, учет Методики ФСТЭК России).

Предлагаемый подход к автоматизации оценки уровня критичности уязвимостей программных и программно-аппаратных средств информационных систем с использованием машинного обучения состоит из следующих этапов:

1. Выбор существенных свойств, характеризующих уязвимости, из некоторого выбранного множества.
2. Разбиение множества уязвимостей на классы по степени их схожести между собой.
3. Подготовка обучающей выборки экспертами.
4. Обучение модели.
5. Классификация уязвимостей по уровню критичности при помощи обученной модели.

Выбор существенных свойств, характеризующих уязвимости, из некоторого выбранного множества. В качестве исходного множества уязвимостей, уровень критичности которых будет оценен применительно к конкретной информационной системе, предлагается использовать текущее содержимое БДУ ФСТЭК России.

Анализ содержимого данного банка свидетельствует о том, что содержащиеся в нем уязвимости описываются следующим полным набором параметров:

- описание уязвимости;
- уязвимое программное обеспечение;
- операционные системы и аппаратные платформы, на которых функционирует программное обеспечение с обнаруженной уязвимостью;
- тип ошибки (в соответствии с CWE);

- класс уязвимости, обнаруженной в программном обеспечении;
- базовый вектор общей системы оценки уязвимости (CVSS);
- базовая оценка CVSS обнаруженной уязвимости и соответствующий уровень опасности;
- возможные меры по устранению уязвимости;
- статус уязвимости;
- наличие эксплойта;
- способ эксплуатации;
- способ устранения;
- информация об устранении;
- ссылки на источники;
- идентификаторы других систем описаний уязвимостей;
- сведения об инцидентах информационной безопасности;
- последствия эксплуатации уязвимости;
- дата публикации;
- дата последнего обновления;
- прочая информация.

Для уязвимостей, содержащихся в БДУ ФСТЭК России, предлагается определить минимальный набор параметров, достаточно полно их характеризующий в контексте решения поставленной задачи.

Исходные данные, применяемые при машинном обучении, часто содержат много признаков (размерностей), среди которых: избыточные (дублируют информацию), слабо информативные (почти не влияют на результат), а также шум (мешают модели обобщать). Уменьшение размерности исходных данных позволяет упростить модель и снизить риск переобучения, ускорить обучение модели, сократить объем памяти для хранения данных, улучшить визуализацию результатов работы модели (например, проекция на 2D/3D), отфильтровать шум и выделить сигнальные шаблоны.

Таким образом к полному набору параметров уязвимостей, содержащихся в БДУ ФСТЭК России, предлагается применить операцию уменьшения их размерности до минимально необходимого количества. Это количество обозначим числом k.

В дальнейшем все уязвимости, с которыми предстоит работать, будем представляться в виде векторов параметров размерности k. При этом к векторам параметров предварительно будут применены операции стандартизации и нормализации, для того чтобы вектора имели одинаковые размерности, параметры разных уязвимостей, имели одинаковый вес, а также для заполнения пустых или ошибочных значений параметров.

Разбиение множества уязвимостей на классы по степени их схожести между собой. Множество уязвимостей, содержащихся в БДУ ФСТЭК России, разобьем на классы при помощи ML-модели, которая настроена для решения задачи кластеризации.

В результате кластеризации множество n всех содержащихся в настоящее время в БДУ ФСТЭК России уязвимостей будет разбито на N классов.

Подготовка обучающей выборки экспертами. На следующем этапе для информационной системы, для которой осуществляется оценка уровня критичности уязвимостей, эксперты подготавливают обучающую выборку для последующего обучения модели.

Количество уязвимостей, которое должно быть взято экспертами из каждого из N классов, обозначим m. Обучающая выборка будет представлять собой множество из $m \times N$ уязвимостей, представленных векторами из k существенных параметров, и их уровней критичности. Число m в ходе экспериментов должно быть подобрано для достижения требуемой точности работы модели.

Таким образом, из БДУ ФСТЭК России эксперты выбирают m уязвимостей каждого из N классов и для каждой уязвимости определяют ее уровень критичности V_i, где $i \in [1; m \times N]$ в соответствии с Методикой. Уровень критичности при этом может принимать одно из четырех значений: низкий, средний, высокий и критический.

Обучение модели. Автоматизированную оценку уровня критичности уязвимостей программных и программно-аппаратных средств предлагается осуществлять на основе ML-модели, настроенной на решение задачи классификации.

Полученная от экспертов обучающая выборка используется для обучения ML-модели методом обучения с учителем.

В результате обучения модели будут подобраны такие значения ее параметров, при которых она при подаче на вход уязвимостей, заданных векторами параметров, на выходе будет выдавать уровень их критичности с требуемой точностью.

Классификация уязвимостей по уровню критичности при помощи обученной модели. После обучения на вход обученной ML-модели будем подавать множество остальных известных уязвимостей, в том числе содержащихся в БДУ ФСТЭК России. Модель будет решать типовую задачу классификации подаваемых на ее вход уязвимостей, соотнося их с одним их четырех уровней критичности (низкий, средний, высокий и критический).

Полученная информация может быть использована оператором защищаемой информационной системы в условиях ограниченности временных и человеческих ресурсов для принятия обоснованного решения о необходимости и приоритетности устранения уязвимостей как в текущий момент, так и в дальнейшем, в рамках контроля за появлением новых и изменением характеристик старых уязвимостей.

Ожидаемым результатом от применения предложенного подхода к автоматизации оценки уровня критичности уязвимостей программных и программно-аппаратных средств с использованием машинного обучения является повышение эффективности деятельности экспертов в части:

- увеличения полноты охвата множества уязвимостей за счет повышения процента приоритезированных известных (уже содержащихся в БДУ ФСТЭК России) уязвимостей;
- повышения своевременности за счет сокращения времени на приоритезацию новых (выявленных в ходе мониторинга вновь добавленных в БДУ ФСТЭК России) уязвимостей;
- повышение точности определения уровня критичности уязвимостей в условиях дефицита квалифицированных кадров и за счет снижения субъективности экспертов при оценке частных показателей I_{infr}, I_{at} и I_{imp}.

Следует отметить, что первые четыре этапа предложенного подхода (выбор существенных свойств уязвимостей, разбиение множества уязвимостей на классы по степени их схожести между собой, подготовка обучающей выборки и обучение модели) потребуют существенных временных затрат со стороны экспертов разово. Кроме того, указанная работа в условиях дефицита собственных квалифицированных кадров у оператора информационной системы может быть выполнена с привлечением сторонних специалистов.

Конкретные числовые значения, подтверждающие ожидаемое повышение эффективности оценки уровня критичности уязвимостей при применении предложенного подхода, планируется получить в ходе практических экспериментов с применением специализированной стендовой ПЭВМ.

Практическую реализацию предложенного подхода предполагается осуществить в 5 этапов:

1. Получение, первичный анализ и преобразование исходных данных об уязвимостях. В качестве исходных данных предполагается использовать множество уязвимостей, содержащихся в БДУ ФСТЭК России, а также результаты оценки уровня критичности уязвимостей, полученные экспертами в соответствии с Методикой ФСТЭК России.
2. Выбор моделей машинного обучения, наиболее подходящих для решения поставленной задачи. На основании публикаций авторов, описывающих решение сходной задачи [12,13,18], в рамках практической реализации предлагаемого подхода предполагается использовать модель для обработки естественного языка BERT в сочетании с моделью, реализующей метод машинного обучения «Случайный лес» (Random Forest). Данный набор, возможно, будет скорректирован по результатам предыдущего этапа.
3. Определение набора программного обеспечения для запуска выбранных моделей и его системных требований. В качестве базового программного окружения для специализированной стендовой ПЭВМ предполагается использовать ОС Windows 10/11, Python 3.8+, менеджер пакетов pip. Для развертывания модели BERT – фреймворки PyTorch или TensorFlow, библиотеки Hugging Face Transformers, Hugging Face Tokenizers и Hugging Face Datasets, а также CUDA Toolkit и cuDNN. Развертывание модели, реализующей алгоритм «Случайный лес», планируется организовать с применением библиотеки Scikit-learn и Pandas.
4. Развертывание аппаратных средств с установленными характеристиками и их настройка. Предварительные характеристики специализированной стендовой ПЭВМ, достаточные для практической реализации предложенного подхода: оперативная память – 16 ГБ, процессор – не менее 4 ядер с поддержкой набора инструкций AVX, накопитель – от 10 ГБ свободного пространства, видеокарта – от NVIDIA серии GTX 1060, RTX 2060/3060 и выше, содержащая от 11 ГБ видеопамяти.
5. Проведение экспериментов. На данном этапе предполагается проведение экспериментов по автоматизированной оценке уровня критичности уязвимостей программных и программно-аппаратных средств, с целью достижения целевых значений показателей эффективности. При этом может потребоваться дополнение и (или) корректировка обучающей выборки, дообучение модели, изменение параметров ее функционирования.

Заключение

В результате проведенного исследования:

- подчеркнута значимость оценки уровня критичности уязвимостей программных, программно-аппаратных средств как одного из ключевых

элементов обеспечения безопасности информационных систем;
- обозначены сложности практического применения методики оценки уровня критичности уязвимостей программных и программно-аппаратных средств ФСТЭК России от 30 июня 2025 г.;
- предложен вариант преодоления сложностей практического применения Методики путем автоматизации оценки уровня критичности уязвимостей программных, программно-аппаратных средств;
- проведен обзор существующих подходов к автоматизации оценки уровня критичности уязвимостей программных, программно-аппаратных средств;
- предложен инновационный подход к автоматизации оценки уровня критичности уязвимостей программных, программно-аппаратных средств с использованием машинного обучения, приведено его описание, преимущества, план практической реализации.

Ожидаемым результатом от применения предложенного подхода к автоматизации оценки уровня критичности уязвимостей программных, программно-аппаратных средств с использованием машинного обучения является повышение эффективности работы специалистов по информационной безопасности в части увеличения полноты охвата множества уязвимостей, повышения своевременности и точности определения уровня критичности уязвимостей без использования громоздких, дорогостоящих, сложных в освоении и эксплуатации систем класса SGRC.

Следует отметить, что хотя применение описанного подхода к автоматизации оценки уровня критичности уязвимостей программных и программно-аппаратных средств с использованием машинного обучения и не избавляет операторов информационных систем от необходимости расчетов в соответствии с Методикой для обеспечения отчетности перед регулятором, но позволяет повысить эффективность фактической защищенности информационных систем от угроз информационной безопасности в современных реалиях.

Одним из перспективных направлений возможного развития предложенного подхода видится дополнительное использование в качестве входных данных, помимо БДУ ФСТЭК России, информации об уязвимостях из альтернативных систем описания уязвимостей. Для обеспечения возможности обработки таких уязвимостей предварительно необходимо будет представить их в виде векторов параметров, соответствующих тем, которые используются в БДУ ФСТЭК России. К полученным векторам параметров должны быть применены операции стандартизации и нормализации.

Другим направлением совершенствования предложенного подхода является разработка средств автоматизации контроля за появлением в БДУ ФСТЭК России, на официальных информационных ресурсах разработчиков программного обеспечения и программно-аппаратных средств и исследователей в области информационной безопасности, а также в их иных источниках, содержащих сведения об известных уязвимостях, информации о новых уязвимостях, а также изменениях характеристик ранее описанных уязвимостей. Помимо собственно контроля такие средства могли бы обладать функцией автоматизированной загрузки информации об уязвимостях, стандартизации и нормализации их параметров, автоматизированного определения уровня их критичности, а также оповещения специалистов оператора информационной системы.

Литература

1. Ефимов А.О. Причины возникновения, классификация и критичность уязвимостей программного обеспечения информационных систем // Вестник Дагестанского государственного технического университета. Технические науки. 2025. Т. 52. № 2. С. 98–106.
2. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств : методический документ / утв. ФСТЭК России 30 июня 2025 г. // ФСТЭК России. URL: https://fstec.ru/files/ …---30--2025-.pdf (дата обращения: 28.06.2026).
3. Заведенская А. Обзор изменений в законодательстве. Июль, август 2025 г. // IT Security Russia. 2025. № 4. URL: https://www.itsec.ru/articles/obzor-izmenenij-v-zakonodatelstve-iyul-avgust-2025 (дата обращения: 28.06.2026).
4. Оценка уязвимостей: как выявлять и устранять слабые места в кибербезопасности // SecurityLab. 2025. 16 апреля. URL: https://www.securitylab.ru/ …558284.php (дата обращения: 02.01.2026).
5. Намиот Д.Е. О кибератаках с помощью систем искусственного интеллекта // International Journal of Open Information Technologies. – 2024. Vol. 12, No. 9. P. 132-141. URL: https://injoit.org/index.php/j1/article/view/1958/1776 (дата обращения: 28.06.2026).
6. Крюков С. ИИ ускорил атаки быстрее, чем компании успели перестроить защиту // Hi-

Tech Mail. 2026. 30 января. URL: https://hi-tech.mail.ru/articles/ …zashitu/ (дата обращения: 03.07.2026).
7. Могилко И.А. Программное средство для анализа и мониторинга уязвимостей в соответствии с банком данных угроз безопасности информации ФСТЭК РФ // Вестник науки. 2025. Т. 2. № 7 (88). С. 272-279.
8. Уровни критичности уязвимостей // Солар. 2025. 27 февраля. URL: https://rt-solar.ru/ … blog/5318/ (дата обращения: 02.01.2026).
9. Жуков В.Г., Селигеев С.В. Автоматизация оценки уязвимостей программных, программно-аппаратных средств в целевой информационной системе // Прикаспийский журнал: управление и высокие технологии. 2023. № 4 (64). С. 16-25. URL: https://cyberleninka.ru/article/n/avtomatizatsiya-otsenki-uyazvimostey-programmnyh-programmno-apparatnyh-sredstv-v-tselevoy-informatsionnoy-sisteme (дата обращения: 11.02.2026).
10. ГОСТ Р 71476-2024. Искусственный интеллект. Концепции и терминология искусственного интеллекта. М.: Российский институт стандартизации, 2024. 38 с.
11. Голиков Е., Синицин Ф., Федотов С. и др. Учебник по машинному обучению // Яндекс Образование. URL: https://education.yandex.ru/ … /ml (дата обращения: 28.06.2026).
12. Bonhomme C., Dulaunoy A. VLAI: A RoBERTa-Based Model for Automated Vulnerability Severity Classification. URL: https://arxiv.org/abs/2507.03607 (дата обращения: 28.06.2026).
13. Частикова В.А., Козачек К.В., Согомонян Е.К., Луговой Д.А., Серый Н.В. Методика определения критичности уязвимостей с использованием технологий BERT и Random Forest // Вестник УрФО. Безопасность в информационной среде. 2025. № 2 (56). С. 40-48.
14. VLAI: Automated Vulnerability Severity Classification (Russian Text) URL: https://huggingface.co/ … Roberta-large (дата обращения: 28.06.2026).
15. Ozer M.A., Dündar S. Evaluating LLM Performance on CWE Identification and CVSS Estimation // 2026 5th International Informatics and Software Engineering Conference (IISEC 2026). IEEE, 2026. URL: https://iisec.tbdakademi.org.tr/2026 (дата обращения: 28.06.2026).
16. Torkamani M.J., Ng J., Mehrotra N. et al. CWE and Severity Identification Artifacts // Zenodo. 2025. 1. Jan. URL: https://zenodo.org/records/15555291 (дата обращения: 28.06.2026).
17. Parente F.R., Rodrigues E.B., Mattos C.L. FRAPE: A Framework for Risk Assessment, Prioritization and Explainability of vulnerabilities in cybersecurity // Journal of Information Security and Applications. 2025. Vol. 89. Art. 103971. URL: https://www.sciencedirect.com/science/article/abs/pii/S2214212625000092 (дата обращения: 28.06.2026).
18. Русинова З.Р. Разработка инструмента для автоматического выявления уязвимостей в исходном коде на основе глубоких нейронных сетей: магистерская диссертация: 09.04.02 // Уральский федеральный университет. Екатеринбург, 2024. // Электронный научный архив УрФУ. URL: https://elar.urfu.ru/bitstream/10995/140355/1/m_th_z.r.rusinova_2024.pdf (дата обращения: 28.06.2026).

Тихонов Алексей Юрьевич. Российский государственный университет нефти и газа (национальный исследовательский университет) им. И.М. Губкина, г. Москва, Россия. Ассистент. Область научных интересов: информационные системы, информационная безопасность, технологии искусственного интеллекта. E-mail: aliennet@rambler.ru

A Machine Learning Approach to Automating Vulnerability Severity Assessment

A.Y. Tikhonov
National University of Oil and Gas Gubkin University, Moscow, Russia

Abstract. The article presents the results of a study on improving the efficiency of information security specialists in assessing the criticality level of vulnerabilities in software and hardware-software systems. The importance of this activity for the comprehensive security of information systems is emphasized, and the results of a review of existing solutions for improving its efficiency through automation are provided. An approach to automating the assessment of vulnerability criticality using machine learning is proposed; its description, advantages, and a practical implementation plan are presented. In conclusion, promising directions for further development of the proposed approach are outlined.

Keywords: *artificial intelligence, machine learning, vulnerability, severity level, information system, information security.*
DOI: 10.14357/20790279260314 **EDN:** QPQHJI

References

1. Efimov A.O. Causes, classification and severity of information system software vulnerabilities. *Vestnik Dagestanskogo Gosudarstvennogo Tekhnicheskogo Universiteta. Tekhnicheskie Nauki*. 2025; 52(2):98-106. (In Russ.).
2. *Methodology for Assessing the Severity Level of Vulnerabilities of Software and Software-Hardware Tools: Methodological Document.* FSTEC of Russia. Moscow. 2025. (In Russ.). Available from: https://fstec.ru/files/ …---30--2025-.pdf [Accessed 28 Jun 2026].
3. Zavedenskaya A. Review of legislative changes. July, August 2025. *Information Security*. 2025; (4). (In Russian). Available from: https://www.itsec.ru/articles/obzor-izmenenij-v-zakonodatelstve-iyul-avgust-2025 [Accessed 28 Jun 2026].
4. *Vulnerability assessment: how to identify and eliminate weaknesses in cybersecurity*. SecurityLab, 2025, April 16. (In Russ.). Available from: https://www.securitylab.ru/ …558284.php [Accessed 02 January 2026].
5. Namiot D.E. On cyberattacks using artificial intelligence systems. *International Journal of Open Information Technologies*. 2024; 12(9):132-141. (In Russ.). Available from: https://injoit.org/index.php/j1/article/view/1958/1776 [Accessed 28 Jun 2026].
6. Krykov S. AI accelerated attacks faster than companies managed to rebuild protection. *Hi-Tech Mail*, 2026, January 30. (In Russ.). Available from: https://hi-tech.mail.ru/articles/ …zashitu/ [Accessed 03 July 2026].
7. Mogilko I. A. Software tool for analysis and monitoring of vulnerabilities in accordance with the data bank of information security threats of FSTEC RF. *Vestnik Nauki*. 2025;2(7):272-279. (In Russ.).
8. *Vulnerability severity levels*. Solar, 2025, February 27. (In Russ.). Available from: https://rt-solar.ru/ … blog/5318/ [Accessed 2 January 2026].
9. Zhukov V. G., Seligeev S. V. Automation of vulnerability assessment of software and firmware in the target information system. *Prikaspiyskiy Zhurnal: Upravlenie i Vysokie Tekhnologii*. 2023;4(64):16-25. (In Russ.). Available from: https://cyberleninka.ru/article/n/avtomatizatsiya-otsenki-uyazvimostey-programmnyh-programmno-apparatnyh-sredstv-v-tselevoy-informatsionnoy-sisteme [Accessed 11 February 2026].
10. GOST R 71476-2024. *Artificial intelligence. Artificial intelligence concepts and terminology*. Moscow, Russian Standardization Institute, 2024. p. 38 (In Russ.).
11. Golikov E., Sinitsin F., Fedotov S. et al. Machine Learning Textbook. *Yandex Education*, 2022. (In Russ.). Available from: https://education.yandex.ru/ … /ml [Accessed 28 Jun 2026].
12. Bonhomme C., Dulaunoy A. *VLAI: A RoBERTa-Based Model for Automated Vulnerability Severity Classification.* Available from: https://arxiv.org/abs/2507.03607 [Accessed 28 Jun 2026].
13. Chastikova V.A., Kozachek K.V., Sogomonyan E.K. et al. Methodology for determining vulnerability severity using BERT and Random Forest technologies. *Vestnik UrFO. Bezopasnost v Informatsionnoy Sfere*. 2025;2(56):40-48. (In Russ.).
14. *VLAI: Automated Vulnerability Severity Classification (Russian Text)*. Available from: https://huggingface.co/ … Roberta-large [Accessed 28 Jun 2026].
15. Ozer M. A., Dündar S. Evaluating LLM Performance on CWE Identification and CVSS

Estimation. 2026. *5th International Informatics and Software Engineering Conference (IISEC 2026)*. IEEE, 2026. Available from: https://iisec.tbdakademi.org.tr/2026 [Accessed 28 Jun 2026].
16. Torkamani M. J., Ng J., Mehrotra N. et al. CWE and Severity Identification Artifacts. *Zenodo*; 2025. Available from: https://zenodo.org/records/15555291 [Accessed 28 Jun 2026].
17. Parente F.R., Rodrigues E.B., Mattos C.L. FRAPE: A Framework for Risk Assessment, Prioritization and Explainability of vulnerabilities in cybersecurity. *Journal of Information Security and Applications*. 2025;(89):103971. Available from: https://www.sciencedirect.com/science/article/abs/pii/S2214212625000092 [Accessed 28 Jun 2026].
18. Rusinova Z. R. Development of a Tool for Automatic Detection of Vulnerabilities in the Source Code Based on Deep Neural Networks: Master's thesis. *Ural Federal University, Ekaterinburg*, 2024. (In Russ.). Available from: https://elar.urfu.ru/bitstream/10995/140355/1/m_th_z.r.rusinova_2024.pdf [Accessed 28 Jun 2026].

Tikhonov Alexey Y. Assistant, National University of Oil and Gas Gubkin University, 65 Leninsky ave., Moscow, 119991, Russia. E-mail: aliennet@rambler.ru