УДК 004.056.53:336.71
DOI: 10.17277/vestnik.2026.03.pp.436-451

КОМПЛЕКСНЫЙ АНАЛИЗ ПРИМЕНИМОСТИ МЕТОДОВ ОБНАРУЖЕНИЯ DDoS-АТАК В SDN-ИНФРАСТРУКТУРЕ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ С УЧЕТОМ АКТУАЛЬНОЙ РОССИЙСКОЙ РЕГУЛЯТОРНОЙ БАЗЫ И ОТКРЫТЫХ ДАННЫХ

© В. В. Бритвина[1,2] ✉, Г. П. Конюхова[3], Е. О. Боброва[4], М. А. Иванов[4], А. О. Гусев[4], Ж. В. Мекшенева[2], О. В. Дубровина[5]

[1] *Кафедра «Инфокогнитивные технологии», Saaturn2026@mail.ru; ФГАОУ ВО «Московский политехнический университет», Москва, Российская Федерация;*
[2] *кафедра «Прикладная математика», АНО ВО «Московский университет «Синергия», Москва, Российская Федерация;*
[3] *кафедра «Управление и информатика в технических системах», ФГАОУ ВО «МГТУ «СТАНКИН», Москва, Российская Федерация;*
[4] *кафедра «Информационная безопасность», ФГАОУ ВО «Московский политехнический университет», Москва, Российская Федерация;*
[5] *Многопрофильный колледж*, *ФГБОУ ВО «ТГТУ», Тамбов, Российская Федерация*

Ключевые слова: обнаружение атак; открытые датасеты; программно-определяемые сети; регуляторное соответствие; финансовые организации; DDoS-атаки; Random Forest; XGBoost.

Аннотация: Рассмотрена задача оценки применимости методов обнаружения DDoS-атак в SDN-инфраструктуре финансовых организаций. Актуальность исследования обусловлена высокой значимостью атак типа «отказ в обслуживании» для обеспечения доступности цифровых сервисов, а также повышенной критичностью контроллера и каналов управления в программно-определяемых сетях. Проведен сравнительный анализ методов машинного обучения, глубокого обучения и ансамблевых моделей по трем группам критериев: качество обнаружения, воспроизводимость и регуляторно-эксплуатационная применимость. Показано, что методы семейства Random Forest и XGBoost-подобные ансамбли обеспечивают рациональный баланс между точностью, объяснимостью, скоростью инференса и удобством интеграции в контуры SIEM/SOC. Отмечено, что наиболее сложные deep-модели могут демонстрировать высокие лабораторные метрики, однако уступают интерпретируемым ансамблевым методам по воспроизводимости, аудируемости и эксплуатационной зрелости. Сделан вывод о необходимости оценивать методы обнаружения DDoS-атак не только по Accuracy и F1-score, но и по совокупности критериев, связанных с открытостью данных, переносимостью результатов и соответствием требованиям регулируемой финансовой инфраструктуры.

Введение

Программно-определяемые сети (*англ*. Software Defined Networks (SDN)) продолжают рассматриваться как одна из базовых архитектур для гибкого управления сетевой инфраструктурой, включая сегментацию, программируемое рас-

пределение правил и централизованный контроль [1]. Для финансовых организаций преимущества SDN сочетаются с очевидной уязвимостью: контроллер и каналы управления становятся критически важными элементами, нарушение доступности которых способно повлиять как на защиту информации, так и на непрерывность платежных и клиентских сервисов [2 – 4].

Вопросы архитектурной устойчивости и сохранения работоспособности цифровых систем при сбоях дополнительно подчеркивают значимость системного подхода к реализации отказоустойчивости программного обеспечения и инфраструктуры [5].

В ряде более ранних работ по данной теме основной акцент делался на собственные математические модели и экспериментальные метрики. Однако такой подход неизбежно вызывает вопросы о воспроизводимости результатов, если не представлены полный стенд, исходные журналы и программный код. Поэтому в настоящей статье тема сформулирована как комплексный анализ применимости методов обнаружения DDoS-атак, а аналитическая часть построена на двух опорах: официальной российской регуляторной базе и открытых данных с опубликованными результатами исследований.

Цель статьи – сформировать воспроизводимую схему оценки применимости методов обнаружения DDoS-атак в финансовой SDN-инфраструктуре и на этой основе определить методы, наиболее целесообразные для практического внедрения.

Материалы и методы

Методическая схема исследования построена как воспроизводимый аналитический обзор, в котором сопоставление методов обнаружения DDoS-атак выполняется не на основе закрытого экспериментального стенда, а на базе официальных документов, открытых датасетов и опубликованных результатов рецензируемых работ. Такой подход выбран сознательно, поскольку для финансовой организации значение имеют не только максимальные лабораторные метрики, но и проверяемость источников, переносимость выводов и возможность независимой верификации результатов в рамках внутреннего контроля и аудита.

В качестве эмпирической базы использованы три группы источников. Первая группа включает официальную статистику Банка России по компьютерным атакам и инцидентам операционной надежности в финансовой сфере за 2024 год [6], она позволяет обосновать практическую значимость DDoS-угроз именно для банковского и платежного контура. Вторая группа охватывает публичные датасеты CICDDoS2019 [7] и InSDN [8], которые служат воспроизводимой основой для сопоставления методов по потоковым признакам и по SDN-специфичным сценариям атак [9, 10]. Третья группа состоит из современных публикаций, в которых результаты для различных моделей приведены на открытых данных и представлены в сопоставимой форме.

Сравнение методов проводилось по трем измерениям. Первое измерение характеризует качество обнаружения и включает показатели Accuracy, Precision, Recall и F1-score, то есть стандартный набор метрик для задач бинарной и многоклассовой классификации сетевых атак. Второе измерение отражает охват и воспроизводимость результатов: приоритет отдается подходам, протестированным на нескольких публичных датасетах, так как это снижает риск переобучения на особенностях единственного набора данных и повышает доверие к выводам. Третье измерение описывает регуляторно-эксплуатационную применимость, то есть совместимость метода с требованиями ГОСТ Р 57580.1–2017, Положений Банка России № 851-П и № 821-П, а также с методикой оценки угроз ФСТЭК России от 05.02.2021 [11 – 14].

При интерпретации результатов отдельно учитывались факторы объяснимости, возможности работы на flow-level признаках, латентности инференса, сложности дообучения и удобства интеграции в контур SIEM/SOC. Для финансовой организации эти характеристики критичны, поскольку даже формально высокая точность алгоритма не гарантирует его пригодность к эксплуатации, если решение трудно сопровождать, невозможно объяснить аудитору или нельзя внедрить в near real-time режим без существенной перестройки инфраструктуры.

Ограничением исследования является отсутствие закрытых корпоративных телеметрических данных конкретной финансовой организации. Однако именно это ограничение делает выводы более универсальными: они опираются на открыто верифицируемую базу и могут быть использованы как стартовая рамка для последующей локальной валидации на внутренних потоках трафика, журналах контроллера SDN и событиях средств защиты. Следовательно, предложенная методика не подменяет пилотное внедрение, а задает прозрачную и реплицируемую процедуру предварительного выбора наиболее перспективных методов.

Дополнительно в работе применяется принцип содержательной интерпретации количественных показателей. Различия между значениями Accuracy и F1-score в пределах десятых и сотых долей процента рассматриваются не как достаточное основание для безусловного выбора метода, а как часть более широкой картины, в которую входят воспроизводимость, объяснимость и эксплуатационные ограничения. Такой подход особенно важен для регулируемой среды финансового сектора, где решение должно быть не только эффективным на тестовых данных, но и управляемым в реальном контуре защиты информации.

Итоговая процедура оценки включает последовательное сопоставление источников угроз, признакового пространства, опубликованных метрик, сценариев внедрения и требований нормативной базы. При формировании перечня альтернатив учитывались дополнительные обзорные и прикладные работы по машинному и глубокому обучению для обнаружения DDoS-атак в SDN-среде [15 – 31]. За счет этого методика может использоваться как шаблон для первичной фильтрации подходов перед построением пилотного стенда и подготовкой программы локальных испытаний в банковской SDN-инфраструктуре.

Результаты и обсуждение

Актуальность угрозы DDoS для финансовых организаций и регуляторная база

По данным Банка России, в 2024 году через автоматизированную систему обработки инцидентов (**АСОИ**) ФинЦЕРТ получено более 750 сообщений о фактах компьютерных атак и компьютерных инцидентов в финансовой сфере [6]. Основными типами атак стали DDoS-атаки, компрометация учетных данных и вредоносное программное обеспечение. Доля атак типа «отказ в обслуживании» составила 39,49 % – почти две пятых от общего объема компьютерных угроз, направленных на финансовый сектор (рис. 1).

Не менее важен операционный аспект. Банк России указывает, что в 2024 году было выявлено более 1500 событий, предположительно связанных со сбоями на технологических участках; 680 из них подтверждены как реальные сбои, а 429 отнесены к инцидентам операционной надежности (**ИОН**). При этом 13,2 % таких ИОН были вызваны компьютерными атаками, в том числе DDoS-атаками. Распределение ИОН по ключевым технологическим процессам показано на рис. 2.

Совокупность приведенных данных свидетельствует о том, что DDoS занимает ведущее место в распределении атак на финансовый сектор и непосредственно влияет на критичные цифровые сервисы. Это означает, что выбор метода

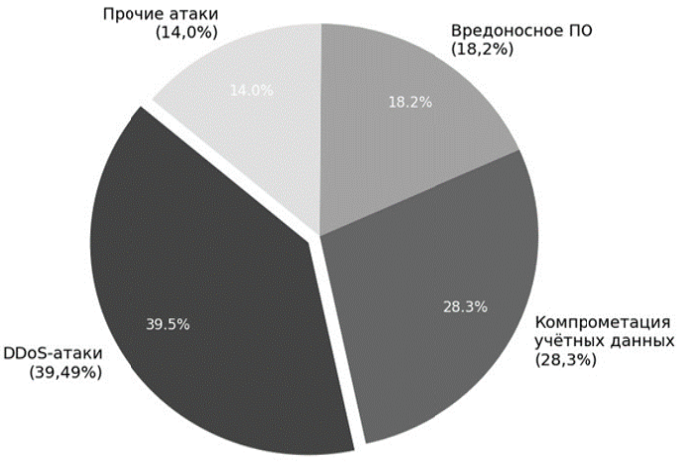

Рис. 1. Распределение типов компьютерных атак в финансовой сфере (Банк России, 2024)

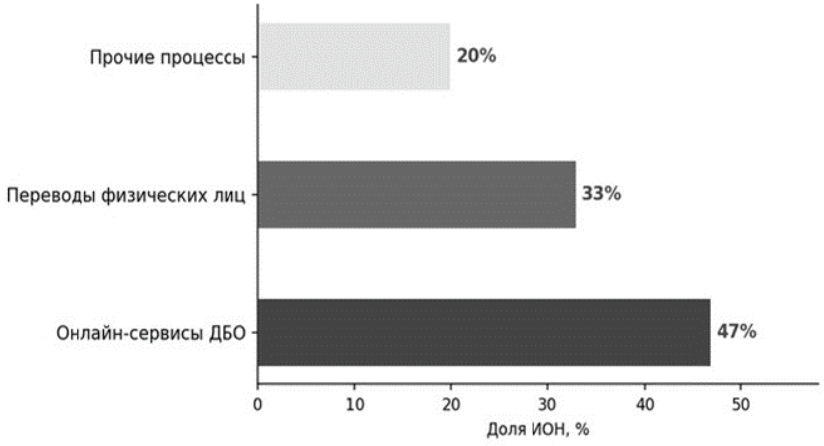

Рис. 2. Распределение инцидентов операционной надежности по затронутым технологическим процессам (Банк России, 2024)

детекции нельзя сводить только к максимизации точности на одном датасете: необходима явная связь с требованиями по доступности сервисов и регуляторному контролю.

Актуальная российская регуляторная база включает как минимум четыре блока: ГОСТ Р 57580.1–2017, Положение Банка России № 851-П, Положение Банка России № 821-П и методику оценки угроз ФСТЭК России от 05.02.2021 [11 – 14] (табл. 1). Положение № 851-П применяется с 29 марта 2025 года и заменило Положение № 683-П; Положение № 821-П вступило в силу с 1 апреля 2024 года, при этом Положение № 719-П признано утратившим силу.

Открытые данные для анализа применимости методов

Для анализа применимости методов в статье использованы не закрытые внутренние выборки, а открытые данные и публикации, опирающиеся на публичные SDN-датасеты. Это обеспечивает более высокую воспроизводимость результатов и позволяет честно разделить первичные входные данные и аналитические выводы.

Таблица 1

Актуальные нормативные документы и их роль в анализе применимости методов

Документ	Смысл для финансовой организации	Что дает для анализа методов
ГОСТ Р 57580.1–2017	Базовый отраслевой стандарт защиты информации финансовых организаций	Требует, чтобы решение поддерживало мониторинг, регистрацию событий и управляемость мер защиты
Положение Банка России № 851-П	Актуальный документ, устанавливающий обязательные требования к защите информации при осуществлении банковской деятельности; применяется с 29.03.2025	Подталкивает к использованию методов, пригодных для встраивания в реальный банковский контур защиты, мониторинга и аудита
Положение Банка России № 821-П	Актуальный документ по защите информации при переводах; действует с 01.04.2024, при этом 719-П утратило силу	Сдвигает акцент с абстрактной точности на устойчивость, контролируемость и проверяемость решения
Методика оценки угроз ФСТЭК России, 2021	Задает порядок и содержание работ по определению угроз безопасности информации	Позволяет трактовать DDoS как угрозу, влияющую не только на ИБ, но и на непрерывность критичных сервисов

Официальная страница CICDDoS2019 указывает, что датасет содержит как легитимный трафик, так и современные DDoS-атаки, а также результаты анализа сетевого трафика в формате CSV с признаками, извлеченными CICFlowMeter-V3. На этапе моделирования фонового трафика авторы использовали поведенческие профили 25 пользователей на базе HTTP, HTTPS, FTP, SSH и e-mail [7].

Наряду с CICDDoS2019 в SDN-литературе широко используется набор InSDN – публично доступный SDN-датасет, включающий нормальный трафик и различные классы атак, специфичных для элементов платформы SDN [8, 9] (табл. 2).

Сравнительный анализ методов обнаружения DDoS-атак в SDN

Систематизация результатов из научной литературы выполняется по трем измерениям: качеству обнаружения на открытых данных, охвату и воспроизводимости на публичных датасетах, а также совместимости с регуляторными и эксплуатационными требованиями финансовой организации.

Первое измерение – качество обнаружения. Стандартными метриками оценки классификаторов в задаче обнаружения DDoS-атак являются Accuracy (доля верно классифицированных образцов), Precision (точность), Recall (полнота) и F1-score (гармоническое среднее Precision и Recall):

Таблица 2

Открытые данные и публикации, использованные в анализе применимости

Набор данных	Подтвержденные открытые характеристики	Почему важен	Ограничения
CICDDoS2019	Открытый набор UNB; PCAP + CSV; CICFlowMeter-V3; 25 профилей; современные DDoS [7]	Воспроизводимая основа для анализа потоковых признаков	Не является специфически банковским
InSDN	Публично доступный SDN-датасет; нормальный трафик и SDN-специфичные классы атак [8, 9]	Опорный бенчмарк в SDN-литературе	Часть публикаций привязана только к InSDN
Много-контроллерные наборы	Собственные стенды; XGBoost показал 98,5 % при test time 70 мс [29]	Оценка эксплуатационных компромиссов	Хуже воспроизводимы, чем открытые бенчмарки

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}};$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}};$$

$$F_1 = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}},$$

где TP – истинно положительные результаты; FP – ложноположительные; FN – ложноотрицательные [15]. Опубликованные значения метрик для рассматриваемых методов на открытых SDN-датасетах приведены в табл. 3 и на рис. 3.

Плотная концентрация значений Accuracy в диапазоне 98 – 100 % свидетельствует о высокой зрелости направления. Вместе с тем именно поэтому чисто «метрическое» сравнение недостаточно для прикладного вывода: различия в десятых и сотых долях процента практически неразличимы в реальных условиях эксплуатации и не позволяют однозначно выбрать метод без учета второго и третьего измерений.

Второе измерение – охват и воспроизводимость. Методы, верифицированные на нескольких публичных датасетах (InSDN, CICDDoS2019, CICDoS2017), демонстрируют более высокую обобщающую способность по сравнению с методами, протестированными на единственном наборе данных.

Третье измерение – регуляторно-эксплуатационная применимость (табл. 4, рис. 4). Для финансовой организации, работающей в рамках ГОСТ Р 57580.1–2017, Положений № 851-П и № 821-П, существенны следующие критерии: совместимость с flow-level признаками и SDN-телеметрией; объяснимость результатов для аудита и внутреннего контроля; пригодность к near real-time внедрению; простота периодического дообучения; удобство интеграции с SIEM/SOC [11 – 14]. Из сопоставления следует, что методы OvR + RF и RF удовлетворяют всем пяти критериям применимости при высокой точности. GWO + LightGBM занимает промежуточную позицию: сочетает near real-time инференс с частичной объяснимостью. FedLAD выделяется охватом трех публичных датасетов, что повышает воспроизводимость оценок, однако архитектура федеративного обучения усложняет

Таблица 3

Опубликованные метрики методов на открытых SDN-датасетах

Метод	Датасет(ы)	Accuracy, %	Precision	Recall	F1	Источник
RF (2023)	InSDN	98,72	98,7	98,7	98,7	Batool et al. [10]
GWO+LGBM (2023)	InSDN	99,80	99,8	99,8	99,8	
S-DATE/D-SEM (2024)	InSDN, IoTID-20, UNSWNB-15	98,90	98,9	98,9	98,9	
MDDCC (2024)	InSDN	99,24	99,2	99,2	99,2	
FedLAD (2025)	InSDN, CICDDoS2019, CICDoS2017	98,07	98,1	98,1	98,1	
Transformer (2024)	InSDN	99,02	99,0	99,0	99,0	
DLTHF (2025)	InSDN	99,97	99,97	99,97	99,97	
OvR+RF (2024)	InSDN	99,99	99,99	99,99	99,99	

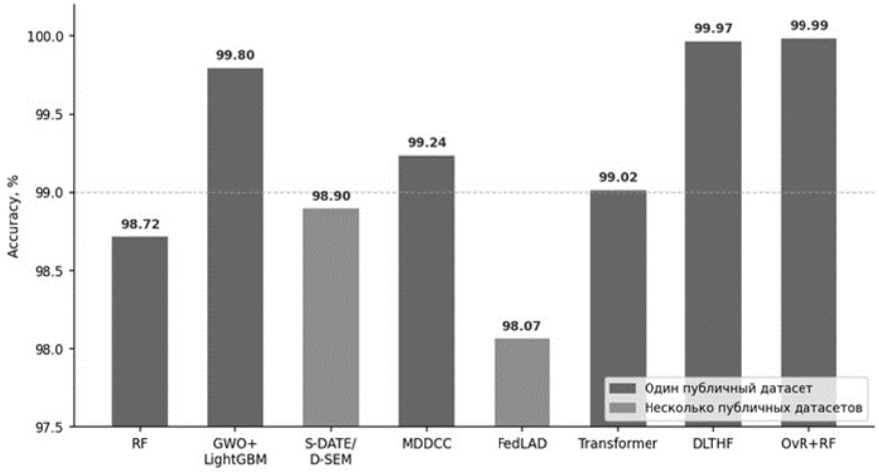

Рис. 3. Опубликованные значения Accuracy методов обнаружения DDoS-атак на открытых SDN-датасетах; отдельной заливкой отмечены методы, верифицированные на нескольких публичных датасетах

сопровождение. Deep-модели (DLTHF, Transformer, MDDCC), несмотря на очень высокую точность, характеризуются низкой объяснимостью и непригодны к near-real-time применению без специализированной инфраструктуры.

Отдельный аргумент в пользу XGBoost-подобных решений дает исследование Sapkota et al. [29], где XGBoost показал оптимальный баланс точности и скорости. Сравнение времени классификации приведено на рис. 5.

Таблица 4

Качественная оценка регуляторно-эксплуатационной применимости методов

Метод	Flow-признаки	Объяснимость/ аудит	NRT	Дообучение	SIEM/ SOC	Характеристика
OvR + RF	Да	Да	Да	Да	Да	Высокая по всем критериям
RF	Да	Да	Да	Да	Да	
GWO + + LGBM	Да	Частично	Да	Да	Да	Хорошая, ограничена объяснимость
FedLAD	Да	Нет	Да	Нет	Да	Средняя: мультидатасетный охват, сложность сопровождения
S-DATE/ D-SEM	Да	Нет	Нет	Да	Да	Средняя: широкий охват, задержка инференса
Transformer	Да	Нет	Нет	Нет	Да	Ниже средней: слабая аудируемость
DLTHF	Да	Нет	Нет	Нет	Да	Ниже средней: максимальная точность, минимальная объяснимость
MDDCC	Да	Нет	Нет	Нет	Да	Ниже средней: специализированная архитектура

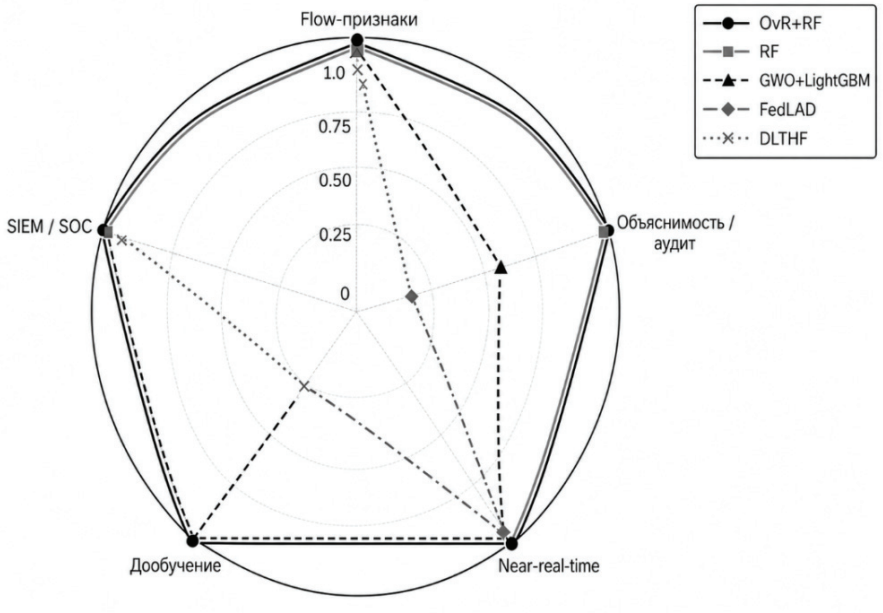

Рис. 4. Профиль регуляторно-эксплуатационной применимости выбранных методов; площадь фигуры соответствует совокупной степени удовлетворения критериев

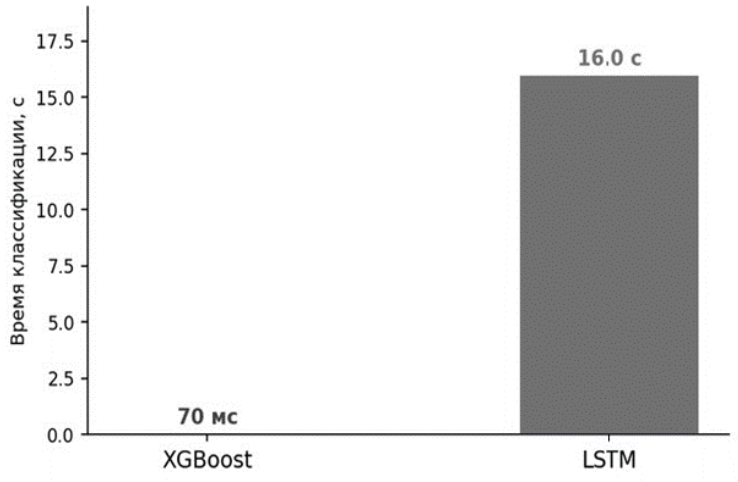

Рис. 5. Сравнение времени классификации тестового массива: XGBoost vs LSTM

Таблица 5

Рекомендуемая поэтапная схема внедрения метода в финансовой организации

Этап	Действия	Измеримые показатели	Практический результат
Пилот	Сбор Flow statistics, журналов контроллера и событий сетевых устройств на ограниченном сегменте	Полнота логов, корректность меток времени, доля потерь телеметрии	Формируется база для честного обучения без подгонки метрик
Сравнение	Параллельная проверка RF/XGBoost/одного гибридного метода на открытых и локальных данных	Accuracy, F1-score на валидации, latency инференса, доля ложных срабатываний	Выбор метода с наилучшим балансом качества и эксплуатации
Интеграция	Связка модели с SIEM, SOC и регламентом реагирования на DDoS	Время детекции, время подтверждения инцидента, доля автоматических действий	Система начинает работать как часть защитного контура
Эксплуатация	Периодическое дообучение, ревизия признаков и уточнение модели угроз	Дрейф модели, обновление датасета, частота корректировки правил	Поддерживается устойчивость решения при изменении профиля трафика и угроз

Рекомендуемая архитектура и практическая схема внедрения

На основании сравнительного анализа можно сформулировать прикладной вывод: наиболее реалистичным стартовым вариантом для финансовой организации является не самая сложная deep-модель, а интерпретируемый ансамблевый или деревообразный подход, встроенный в контур SDN-телеметрии, SIEM и SOC.

Переход от пилотного сегмента к полному контуру защиты требует не только достижения приемлемых значений Accuracy и F1-score, но и подтверждения работоспособности системы в условиях реального трафика финансовой организации. Именно поэтому этапы интеграции и эксплуатации в табл. 5 включают показатели, связанные с временем детекции и поведением модели при дрейфе трафика.

Заключение

Рассмотрена задача оценки применимости методов обнаружения DDoS-атак в SDN-инфраструктуре финансовых организаций. Показано, что для регулируемой финансовой среды выбор метода детекции не должен основываться только на максимальных значениях Accuracy или F1-score, полученных в лабораторных условиях. Существенное значение имеют воспроизводимость результатов, объяснимость срабатываний, скорость инференса, возможность аудита и интеграция с действующими процессами мониторинга и реагирования.

На основании анализа открытых наборов данных CICDDoS2019 и InSDN, опубликованных результатов исследований и требований российской регуляторной базы сделаны следующие выводы:

– использование открытых датасетов позволяет сформировать воспроизводимую основу предварительного сравнения методов обнаружения DDoS-атак, однако не заменяет локальную валидацию на потоках трафика, журналах SDN-контроллера и событиях средств защиты конкретной финансовой организации;

– методы семейства Random Forest и XGBoost-подобные ансамбли обладают наибольшим практическим потенциалом для первичного внедрения, поскольку сочетают высокое качество обнаружения с интерпретируемостью, сравнительно низкой задержкой инференса и удобством интеграции в контуры SIEM/SOC;

– глубокие и гибридные модели могут демонстрировать более высокие значения метрик на отдельных наборах данных, но их применение в финансовой организации требует дополнительного обоснования с точки зрения объяснимости, устойчивости к изменению профиля трафика, трудоемкости сопровождения и готовности инфраструктуры;

– предложенная схема оценки позволяет сократить риск выбора модели, которая показывает высокие публикационные результаты, но оказывается недостаточно удобной для эксплуатации, внутреннего контроля и последующего аудита.

Практическая значимость работы заключается в формировании прозрачного подхода к отбору методов обнаружения DDoS-атак перед построением пилотного стенда. Предложенная логика сравнения может использоваться для подготовки технических требований к сбору flow-level телеметрии, журналов контроллера, событий сетевых устройств и данных средств защиты, а также для согласования критериев оценки между подразделениями информационной безопасности, эксплуатации, SOC и внутреннего аудита.

Дальнейшее развитие исследования целесообразно связать с экспериментальной проверкой выбранных методов на локальных данных финансовой организации, оценкой доли ложных срабатываний в условиях реального трафика, анализом устойчивости моделей к дрейфу признаков и разработкой регламента периодического дообучения. Такой этап позволит перейти от аналитического отбора перспективных подходов к их практической апробации в банковской SDN-инфраструктуре.

Список литературы

1. Software-Defined Networking: A Comprehensive Survey / D. Kreutz, F. M. V. Ramos, P. Verissimo [et al.] // Proceedings of the IEEE. – 2015. – Vol. 103, No. 1. – P. 14–76. doi: 10.1109/JPROC.2014.2371999

2. Dupont, B. The cyber-resilience of financial institutions: significance and applicability / B. Dupont // Journal of Cybersecurity. – 2019. – Vol. 5, Iss. 1. – Art. tyz013. doi: 10.1093/cybsec/tyz013

3. Smaga, P. Profiling the victim – cyber risk in commercial banks / P. Smaga // Computers & Security. – 2025. – Vol. 150. – Art. 104274. doi: 10.1016/j.cose.2024.104274

4. Smaga, P. Evaluating cyber attacks on central banks - identification of trends in cyber threat landscape / P. Smaga // Computers & Security. – 2026. – Vol. 160. – Art. 104742. doi: 10.1016/j.cose.2025.104742

5. Ншот, А. Ф. В. Анализ отказоустойчивости программного обеспечения в архитектуре цифрового предприятия: системный подход / А. Ф. В. Ншот, Г. П. Конюхова, В. В. Бритвина // Вестник ГГНТУ. Технические науки. – 2025. – Т. 21, № 3 (41). – С. 31–37.

6. Банк России. Обзор основных типов компьютерных атак в финансовой сфере в 2024 году. – Москва : Банк России, 2025. – Текст : электронный. – URL : https://www.cbr.ru/collection/collection/file/55129/attack_2024.pdf (дата обращения: 05.05.2026).

7. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy / I. Sharafaldin, A. H. Lashkari, S. Hakak, A. A. Ghorbani // 2019 International Carnahan Conference on Security Technology (ICCST). – 2019. – P. 1–8. doi: 10.1109/CCST.2019.8888419

8. InSDN: A Novel SDN Intrusion Dataset / M. S. Elsayed, N.-A. Le-Khac, S. Dev, A. D. Jurcut // IEEE Access. – 2020. – Vol. 8. – P. 165263–165284. doi: 10.1109/ACCESS.2020.3022633

9. DDoS in SDN: a review of open datasets, attack vectors and mitigation strategies / W. Hill, Y. T. Acquaah, J. Mason [et al.] // Discover Applied Sciences. – 2024. – Vol. 6. – Art. 472. doi: 10.1007/s42452-024-06172-x

10. A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments: Machine Learning, Deep Learning, and Federated Learning Perspectives / S. Batool, M. Aslam, E. Akpokodje, S. F. Jilani // Electronics. – 2025. – Vol. 14, No. 21. – Art. 4222. doi: 10.3390/electronics14214222

11. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. – Москва : Стандартинформ, 2017. – Текст : электронный. – URL : https://docs.cntd.ru/document/1200146534 (дата обращения: 05.05.2026).

12. Банк России. Положение от 30.01.2025 № 851-П «Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента». – Текст : электронный. – URL : https://www.cbr.ru/Queries/UniDbQuery/File/90134/6262 (дата обращения: 05.05.2026).

13. Банк России. Положение от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». – Текст : электронный. – URL : https://www.garant.ru/products/ipo/prime/doc/408082189/ (дата обращения: 05.05.2026).

14. ФСТЭК России. Методика оценки угроз безопасности информации : методический документ от 05.02.2021. – М., 2021. – Текст : электронный. – URL : https://fstec.ru/files/495/---5--2021-/891/---5--2021-.pdf (дата обращения: 05.05.2026).

15. Ali, T. E. Comparison of ML/DL Approaches for Detecting DDoS Attacks in SDN / T. E. Ali, Y.-W. Chong, S. Manickam // Applied Sciences. – 2023. – Vol. 13, No. 5. – Art. 3033. doi: 10.3390/app13053033

16. Ali, T. E. Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review / T. E. Ali, Y.-W. Chong, S. Manickam // Applied Sciences. – 2023. – Vol. 13, No. 5. – Art. 3183. doi: 10.3390/app13053183

17. A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking / A. A. Bahashwan, M. Anbar, S. Manickam [et al.] // Sensors. – 2023. – Vol. 23, No. 9. – Art. 4441. doi: 10.3390/s23094441

18. Comparative Study of AI-Enabled DDoS Detection Technologies in SDN / K.-M. Ko, J.-M. Baek, B.-S. Seo, W.-B. Lee // Applied Sciences. – 2023. – Vol. 13, No. 17. – Art. 9488. doi: 10.3390/app13179488

19. Real-Time Detection of DDoS Attacks Based on Random Forest in SDN / R. Ma, Q. Wang, X. Bu, X. Chen // Applied Sciences. – 2023. – Vol. 13, No. 13. – Art. 7872. doi: 10.3390/app13137872

20. Optimized MLP-CNN Model to Enhance Detecting DDoS Attacks in SDN Environment / M. A. Setitra, M. Fan, B. L. Y. Agbley, Z. E. A. Bensalem // Network. – 2023. – Vol. 3, No. 4. – P. 538–562. doi: 10.3390/network3040024

21. Ensemble Learning Framework for DDoS Detection in SDN-Based SCADA Systems / S. Oyucu, O. Polat, M. Turkoğlu [et al.] // Sensors. – 2024. – Vol. 24, No. 1. – Art. 155. doi: 10.3390/s24010155

22. Detection and mitigation of DDoS attacks based on multi-dimensional characteristics in SDN / K. Wang, Y. Fu, X. Duan, T. Liu // Scientific Reports. – 2024. – Vol. 14. – Art. 16421. doi: 10.1038/s41598-024-66907-z

23. Clinton, U. B. Classification of DDoS attack traffic on SDN network environment using deep learning / U. B. Clinton, N. Hoque, K. R. Singh // Cybersecurity. – 2024. – Vol. 7. – Art. 23. doi: 10.1186/s42400-024-00219-7

24. Songa, A. V. An integrated SDN framework for early detection of DDoS attacks in cloud computing / A. V. Songa, G. R. Karri // Journal of Cloud Computing. – 2024. – Vol. 13. – Art. 74. doi: 10.1186/s13677-024-00625-9

25. Hassan, A. I. An entropy and machine learning based approach for DDoS attacks detection in software defined networks / A. I. Hassan, E. Abd El Reheem, S. K. Guirguis // Scientific Reports. – 2024. – Vol. 14. – Art. 18159. doi: 10.1038/s41598-024-67984-w

26. Wang, H. Overview of DDoS Attack Detection in Software-Defined Networks / H. Wang, Y. Li // IEEE Access. – 2024. – Vol. 12. – P. 38351–38381. doi: 10.1109/ACCESS.2024.3375395.

27. Naeen, H. M. Enhancing SDN security with deep learning and F-balanced cross-entropy for DDoS detection / H. M. Naeen, M. Ghadamyari, M. Barmar // Scientific Reports. – 2025. – Vol. 15. – Art. 33419. doi: 10.1038/s41598-025-18826-w

28. Estupinan Cuesta, E. P. DDoS Attacks Detection in SDN Through Network Traffic Feature Selection and Machine Learning Models / E. P. Estupinan Cuesta, J. C. Martinez Quintero, J. D. Aviles Palma // Telecom. – 2025. – Vol. 6, No. 3. – Art. 69. doi: 10.3390/telecom6030069

29. Machine Learning-Based Attack Detection and Mitigation with Multi-Controller Placement Optimization over SDN Environment / B. Sapkota, A. Ray, M. K. Yadav [et al.] // Journal of Cybersecurity and Privacy. – 2025. – Vol. 5, No. 1. – Art. 10. doi: 10.3390/jcp5010010

30. Ganeshan, S. A Systematic Review of Machine-Learning-Based Detection of DDoS Attacks in Software-Defined Networks / S. Ganeshan, R. K. Ramasamy // Future Internet. – 2026. – Vol. 18, No. 2. – Art. 109. doi: 10.3390/fi18020109

31. A hybrid machine learning approach for detecting DDoS attacks in software-defined networks / I. A. Mahar, K. Aziz, P. Chakrabarti [et al.] // Scientific Reports. – 2026. – Vol. 16. – Art. 6533. doi: 10.1038/s41598-026-35458-w

---

Comprehensive Analysis of the Applicability of DDoS Attack Detection Methods in the SDN Infrastructure of Financial Organizations with Account of the Current Russian Regulatory Framework and Open Data

© **V. V. Britvina[1,2] ✉, G. P. Konyukhova[3], E. O. Bobrova[4], M. A. Ivanov[4], A. O. Gusev[1], Zh. V. Meksheneva[2], O. V. Dubrovina[5]**

[1] *Department of Infocognitive Technologies, Saaturn2026@mail.ru; Moscow Polytechnic University, Moscow, Russian Federation;*
[2] *Department of Applied Mathematics, Moscow Synergy University, Moscow, Russian Federation;*
[3] *Department of Control and Informatics in Technical Systems, STANKIN Moscow State University of Technology, Moscow, Russian Federation;*
[4] *Department of Information Security, Moscow Polytechnic University, Moscow, Russian Federation;*
[5] *Multidisciplinary College, TSTU, Tambov, Russian Federation*

Keywords: attack detection; DDoS attacks; financial organizations; open datasets; Random Forest; regulatory compliance; software-defined networking; XGBoost.

Abstract: This paper examines the applicability of DDoS attack detection methods within the SDN infrastructure of financial institutions. The study is motivated by the significant impact of denial-of-service attacks on the availability of digital services, as well as the critical nature of controllers and control channels in software-defined networks. A comparative analysis of machine learning, deep learning, and ensemble models was conducted based on three groups of criteria: detection performance, reproducibility, and regulatory/operational applicability. The results demonstrate that Random Forest-based methods and XGBoost-style ensembles offer an optimal balance between accuracy, explainability, inference speed, and ease of integration into SIEM/SOC workflows. While highly complex deep learning models may yield impressive metrics in laboratory settings, they often lag behind interpretable ensemble methods in terms of reproducibility, auditability, and operational maturity. The study concludes that DDoS detection methods should be evaluated not only by metrics such as Accuracy and F1-score but also by a comprehensive set of criteria regarding data transparency, result portability, and compliance with the requirements of regulated financial infrastructure.

References

1. Kreutz D., Ramos F.M.V., Verissimo P., Rothenberg C.E., Azodolmolky S., Uhlig S. Software-Defined Networking: A Comprehensive Survey, *Proceedings of the IEEE*, 2015, vol. 103, no. 1, pp. 14-76. doi: 10.1109/JPROC.2014.2371999

2. Dupont B. The cyber-resilience of financial institutions: significance and applicability, *Journal of Cybersecurity*, 2019, vol. 5, iss. 1, art. tyz013. doi: 10.1093/cybsec/tyz013

3. Smaga P. Profiling the victim - cyber risk in commercial banks, *Computers & Security*, 2025, vol. 150, art. 104274. doi: 10.1016/j.cose.2024.104274

4. Smaga P. Evaluating cyber attacks on central banks - identification of trends in cyber threat landscape, *Computers & Security*, 2026, vol. 160, art. 104742. doi: 10.1016/j.cose.2025.104742

5. Nshot A.F.V., Konyukhova G.P., Britvina V.V. [Analysis of software fault tolerance in the architecture of a digital enterprise: a systems approach], *Vestnik GGNTU. Tekhnicheskiye nauki* [Herald of GSTOU. Technical Sciences], 2025, vol. 21, no. 3 (41), pp. 31-37. (In Russ., abstract in Eng.)

6. Available at: https://www.cbr.ru/collection/collection/file/55129/attack_2024.pdf (accessed 05 May 2026).

7. Sharafaldin I., Lashkari A.H., Hakak S., Ghorbani A.A. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy, *2019 International Carnahan Conference on Security Technology* (ICCST), 2019, pp. 1-8. doi: 10.1109/CCST.2019.8888419

8. Elsayed M.S., Le-Khac N.-A., Dev S., Jurcut A.D. InSDN: A Novel SDN Intrusion Dataset, *IEEE Access*, 2020, vol. 8, pp. 165263-165284. doi: 10.1109/ACCESS.2020.3022633

9. Hill W., Acquaah Y.T., Mason J., Limbrick D., Teixeira-Poit S., Coates C., Roy K. DDoS in SDN: a review of open datasets, attack vectors and mitigation strategies, *Discover Applied Sciences*, 2024, vol. 6, art. 472. doi: 10.1007/s42452-024-06172-x

10. Batool S., Aslam M., Akpokodje E., Jilani S. F. A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments: Machine Learning, Deep Learning, and Federated Learning Perspectives, *Electronics*, 2025, vol. 14, no. 21, art. 4222. doi: 10.3390/electronics14214222

11. Available at: https://docs.cntd.ru/document/1200146534 (accessed 05 May 2026).

12. Available at: https://www.cbr.ru/Queries/UniDbQuery/File/90134/6262 (accessed 05 May 2026).

13.Available at: https://www.garant.ru/products/ipo/prime/doc/408082189/ (accessed 05 May 2026).

14. Available at: https://fstec.ru/files/495/---5--2021-/891/---5--2021-.pdf (accessed 05 May 2026).

15. Ali T.E., Chong Y.-W., Manickam S. Comparison of ML/DL Approaches for Detecting DDoS Attacks in SDN, *Applied Sciences*, 2023, vol. 13, no. 5, art. 3033. doi: 10.3390/app13053033

16. Ali T.E., Chong Y.-W., Manickam S. Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review, *Applied Sciences*, 2023, vol. 13, no. 5, art. 3183. doi: 10.3390/app13053183

17. Bahashwan A.A., Anbar M., Manickam S., Al-Amiedy T.A., Aladaileh M.A., Hasbullah I.H. A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking, *Sensors*, 2023, vol. 23, no. 9, art. 4441. doi: 10.3390/s23094441

18. Ko K.-M., Baek J.-M., Seo B.-S., Lee W.-B. Comparative Study of AI-Enabled DDoS Detection Technologies in SDN, *Applied Sciences*, 2023, vol. 13, no. 17, art. 9488. doi: 10.3390/app13179488

19. Ma R., Wang Q., Bu X., Chen X. Real-Time Detection of DDoS Attacks Based on Random Forest in SDN, *Applied Sciences*, 2023, vol. 13, no. 13, art. 7872. doi: 10.3390/app13137872

20. Setitra M.A., Fan M., Agbley B.L.Y., Bensalem Z.E.A. Optimized MLP-CNN Model to Enhance Detecting DDoS Attacks in SDN Environment, *Network*, 2023, vol. 3, no. 4, pp. 538-562. doi: 10.3390/network3040024.

21. Oyucu S., Polat O., Turkoğlu M., Polat H., Aksoz A., Ağdaş M. T. Ensemble Learning Framework for DDoS Detection in SDN-Based SCADA Systems, *Sensors*, 2024, vol. 24, no. 1, art. 155. doi: 10.3390/s24010155

22. Wang K., Fu Y., Duan X., Liu T. Detection and mitigation of DDoS attacks based on multi-dimensional characteristics in SDN, *Scientific Reports*, 2024, vol. 14, art. 16421. doi: 10.1038/s41598-024-66907-z

23. Clinton U.B., Hoque N., Singh K.R. Classification of DDoS attack traffic on SDN network environment using deep learning, *Cybersecurity*, 2024, vol. 7, art. 23. doi: 10.1186/s42400-024-00219-7

24. Songa A.V., Karri G.R. An integrated SDN framework for early detection of DDoS attacks in cloud computing, *Journal of Cloud Computing*, 2024, vol. 13, art. 74. doi: 10.1186/s13677-024-00625-9

25. Hassan A.I., Abd El Reheem E., Guirguis S.K. An entropy and machine learning based approach for DDoS attacks detection in software defined networks, *Scientific Reports*, 2024, vol. 14, art. 18159. doi: 10.1038/s41598-024-67984-w

26. Wang H., Li Y. Overview of DDoS Attack Detection in Software-Defined Networks, *IEEE Access*, 2024, vol. 12, pp. 38351-38381. doi: 10.1109/ACCESS.2024.3375395

27. Naeen H.M., Ghadamyari M., Barmar M. Enhancing SDN security with deep learning and F-balanced cross-entropy for DDoS detection, *Scientific Reports*, 2025, vol. 15, art. 33419. doi: 10.1038/s41598-025-18826-w

28. Estupinan Cuesta E.P., Martinez Quintero J.C., Aviles Palma J.D. DDoS Attacks Detection in SDN Through Network Traffic Feature Selection and Machine Learning Models, *Telecom*, 2025, vol. 6, no. 3, art. 69. doi: 10.3390/telecom6030069

29. Sapkota B., Ray A., Yadav M.K., Dawadi B.R., Joshi S.R. Machine Learning-Based Attack Detection and Mitigation with Multi-Controller Placement Optimization over SDN Environment, *Journal of Cybersecurity and Privacy*, 2025, vol. 5, no. 1, art. 10. doi: 10.3390/jcp5010010

30. Ganeshan S., Ramasamy R.K. A Systematic Review of Machine-Learning-Based Detection of DDoS Attacks in Software-Defined Networks, *Future Internet*, 2026, vol. 18, no. 2, art. 109. doi: 10.3390/fi18020109

31. Mahar I.A., Aziz K., Chakrabarti P., Ahmed N., Ladan M., Javed Y. A hybrid machine learning approach for detecting DDoS attacks in software-defined networks, *Scientific Reports*, 2026, vol. 16, art. 6533. doi: 10.1038/s41598-026-35458-w

---

Umfassende Analyse der Anwendbarkeit von DDoS-Angriffserkennungsmethoden in der SDN-Infrastruktur von Finanzinstituten unter Berücksichtigung der aktuellen russischen Regulierungsdatenbank und offener Daten

Zusammenfassung: Diese Arbeit untersucht die Anwendbarkeit von DDoS-Angriffserkennungsmethoden in der SDN-Infrastruktur von Finanzinstituten. Die Relevanz der Studie ergibt sich aus der hohen Bedeutung von Denial-of-Service-Angriffen für die Gewährleistung der Verfügbarkeit digitaler Dienste sowie der erhöhten Kritikalität von Controller und Kontrollkanälen in softwaredefinierten Netzwerken. Es ist eine vergleichende Analyse von Machine-Learning-, Deep-Learning- und Ensemble-Modellen anhand von drei Kriteriengruppen durchgeführt: Erkennungsqualität, Reproduzierbarkeit sowie regulatorische und operative Anwendbarkeit. Es hat sich gezeigt, dass Random-Forest-Methoden und XGBoost-ähnliche Ensembles ein ausgewogenes Verhältnis zwischen Genauigkeit, Erklärbarkeit, Inferenzgeschwindigkeit und einfacher Integration in SIEM/SOC-Frameworks bieten. Es ist festgestellt, dass die komplexesten Deep-Learning-Modelle zwar hohe

Laborwerte erzielen, jedoch hinsichtlich Reproduzierbarkeit, Auditierbarkeit und operativer Reife den interpretierbaren Ensemble-Methoden unterlegen sind. Es ist die Schlussfolgerung gezogen, dass es notwendig ist, Methoden zur Erkennung von DDoS-Angriffen nicht nur anhand der Genauigkeit und des F1-Scores zu bewerten, sondern auch anhand einer Reihe von Kriterien, die mit der Offenheit der Daten, der Übertragbarkeit der Ergebnisse und der Einhaltung der Anforderungen der regulierten Finanzinfrastruktur zusammenhängen.

Analyse complète de l'applicabilité des methodes de détection des DDOS-attacks sur l'infrastructure SDN des entreprises financiers, compte tenu de la base réglemente russe actuelle et des données open source

Résumé: Est examinée la problématique de l'évaluation de l'applicabilité des méthodes de la détection des DDoS dans les infrastructures SDN des organisations financières. L'actualité de cette recherche tient à la haute importance des attaques de type «refus de service» pour garantir l'accessibilité des services numériques, ainsi qu'à la haute sensibilité des contrôleurs et des canaux de commande dans les réseaux définis par programme. Est effectuée une analyse comparative des méthodes d'apprentissage automatique, d'apprentissage profond et des modèles d'ensembles selon trois groupes de critères: qualité de détection, réproductibilité et applicabilité réglementaire et opérationnelle. Est démontré que les méthodes de la famille Random Forest et les ensembles similaires à XGBoost offrent un équilibre rationnel entre précision, explicabilité, vitesse d'inference et facilité d'intégration dans les systèmes SIEM/SOC. Est noté que les modèles de profondeur les plus complexes peuvent afficher des performances élevées en laboratoire, mais sont inférieurs aux méthodes d'ensembles interprétables en termes de répétabilité, audibilité et maturité opérationnelle. Est conclu qu'il est nécessaire d'évaluer les méthodes de détection des DDoS non seulement par Accuracité et F1-score, mais aussi selon un ensemble de critères liés à la transparence des données, à la portabilité des résultats et à la conformité aux exigences des infrastructures financières réglementées.

Авторы: ***Бритвина Валентина Валентиновна*** – кандидат педагогических наук, доцент кафедры «Инфокогнитивные технологии», ФГАОУ ВО «Московский политехнический университет»; доцент кафедры «Прикладная математика», АНО ВО «Московский университет «Синергия», Москва, Российская Федерация; ***Конюхова Галина Петровна*** – кандидат педагогических наук, доцент, доцент кафедры «Управление и информатика в технических системах», *ФГАОУ ВО «МГТУ «СТАНКИН»*, Москва, Российская Федерация; ***Боброва Екатерина Олеговна*** – старший преподаватель кафедры «Информационная безопасность», ФГАОУ ВО «Московский политехнический университет»; ***Иванов Михаил Александрович*** – студент, Московский политехнический университет, Москва, Российская Федерация; ***Гусев Артем Олегович*** – студент, Московский политехнический университет, Москва, Российская Федерация; ***Мекшенева Жанна Вячеславовна*** – кандидат экономических наук, доцент, заведующий кафедрой «Прикладная математика», АНО ВО «Московский университет «Синергия», Москва, Российская Федерация; ***Дубровина Оксана Васильевна*** – преподаватель, Многопрофильный колледж, ФГБОУ ВО «ТГТУ», Тамбов, Российская Федерация.