УДК 004.023 DOI: 10.26102/2310-6018/2021.32.1.003

Применение генеративных состязательных сетей в системах обнаружения аномалий

А.А. Сычугов, М.М. Греков
Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет», Тула, Российская Федерация

Резюме: На сегодняшний день важным инструментом безопасности является система обнаружения вторжений, основанная на сигнатурах известных атак, однако данный метод неэффективен против уязвимостей нулевого дня. Актуальным подходом для нейтрализации ранее неизвестных компьютерных атак и нового вредоносного программного обеспечения является применение систем обнаружения вторжений на основе аномалий. Для построения системы, позволяющей классифицировать поступающие на вход данные, можно использовать алгоритмы машинного обучения. В настоящий момент применение такой системы обнаружения аномалий в реальных условиях недостаточно эффективно, так как велика вероятность ошибки классификации из-за неравномерного распределения данных между классами. Также необходимо учитывать возможность применения злоумышленником состязательных атак для преодоления алгоритмов классификации, вследствие чего реальная атака может быть пропущена детектором. В связи с этим, в данной статье описана задача несбалансированности обучающего набора данных и неустойчивости к состязательным атакам злоумышленников при использовании системы обнаружения аномалий на основе нейронных сетей. В качестве решения предлагается применить алгоритм генеративных состязательных сетей для дополнения малочисленного класса атак сгенерированными образцами, что также позволяет сделать классификатор более устойчивым к состязательным атакам. Рассмотрен алгоритм обучения генератора и дискриминатора, а также приведено описание набора данных NSL-KDD, который предлагается использовать в качестве обучающего и тестового.

Ключевые слова: вредоносное программное обеспечение, системы обнаружения аномалий, несбалансированность данных, генеративные состязательные сети, машинное обучение.

Для цитирования: Сычугов А.А., Греков М.М. Применение генеративных состязательных сетей в системах обнаружения аномалий. *Моделирование, оптимизация и информационные технологии.* 2021;9(1). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=921 DOI: 10.26102/2310-6018/2021.32.1.003.

Application of generative adversarial networks in anomaly detection systems

A.A. Sychugov, M.M. Grekov
Federal state budgetary educational institution of higher education «Tula state university», Tula, Russian Federation

Abstract: Today, intrusion detection system based on signatures of known attacks is an important security tool, but this method is ineffective against zero-day vulnerabilities. Anomaly-based intrusion detection systems are a relevant approach to neutralize previously unknown computer attacks and new malicious software. Machine learning algorithms can be used to build a system that can classify input data. At the moment, using this an anomaly detection system in real conditions is not effective enough, because there is a high probability of classification errors due to the non-uniform distribution of data between classes. It is also necessary to take into account the possibility of adversarial attacks used by an attacker to overcome classification algorithms, as a result of which a real attack can be missed by the

detector. Thereat, this article describes the problem of imbalance in the training dataset and instability to adversarial attacks by intruders when using an anomaly detection system based on neural networks. As a solution, it is proposed to apply an algorithm of generative adversarial networks to supplement a small class of attacks with generated examples, which also makes the classifier more resistant to adversarial attacks. An algorithm for training the generator and discriminator is considered, and a description of the NSL-KDD dataset is given, which is proposed to be used as a training and test one.

Keywords: malware, anomaly detection systems, data imbalance, generative adversarial networks, machine learning.

For citation: Sychugov A.A., Grekov M.M. Application of generative adversarial networks in anomaly detection systems. *Modeling, Optimization and Information Technology*. 2021;9(1). Available from: https://moitvivt.ru/ru/journal/pdf?id=921 DOI: 10.26102/2310-6018/2021.32.1.003 (In Russ).

Введение

В связи с ростом количества компьютерных атак и вредоносного программного обеспечения (ПО) актуальной является задача обнаружения и предотвращения негативного воздействия на электронно-вычислительные ресурсы. Для обнаружения такого рода воздействий в настоящий момент активно используются системы обнаружения вторжений (СОВ).

Система обнаружения вторжений (Intrusion Detection Systems, IDS) – это программное и/или аппаратное средство, которое собирает данные о работе защищаемой компьютерной системы (вычислительной сети), анализирует поступающую информацию на предмет злонамеренных действий или нарушений политики и автоматически посылает предупреждения администратору [1]. По типу объекта мониторинга СОВ классифицируют на сетевые (Network-based IDS), которые отслеживают трафик в сети, и узловые (Host-based IDS) – осуществляют анализ активности одного узла в сети [1, 2]. По типу метода обнаружения различают подходы, основанные на сигнатурах и на аномалиях.

СОВ на основе сигнатуры (подписи) способны детектировать известные уязвимости и шаблоны атак, но из-за быстрого распространения новых типов атак и неизвестного вредоносного ПО такой метод обнаружения становится неэффективным против уязвимостей нулевого дня.

Метод на основе аномалии (эвристический, основанный на поведении) предполагает первоначальный сбор данных о нормальной работе системы, после чего система обнаружения аномалий (СОА) обеспечивает непрерывный анализ и сравнение текущего состояния с базовым нормальным уровнем, и реагируют на отклонения от модели нормальной активности. При обучении СОА актуальным подходом является применение машинного обучения [3,4], которое позволяет автоматически построить модель, обученную на наборе данных.

В области обнаружения аномалий обучающие наборы данных включают в себя информацию о нормальном функционировании, а также содержат сопоставимые по объему данные об атаках. Как правило, в реальности достаточно трудно получить образцы аномалий в необходимом количестве, что вызывает несбалансированность набора данных. Так как целью большинства алгоритмов машинного обучения является минимизация функции ошибки, обученный классификатор склонен отдавать предпочтение доминирующему классу, игнорируя малочисленный класс [5]. Неправильная классификация затрудняет анализ и не позволяет администратору эффективно реагировать на реальные атаки.

Как один из методов машинного обучения для обнаружения аномалий применяются нейронные сети [3], однако необходимо учитывать их неустойчивость к

нестандартным данным, которые генерируются нейронной сетью злоумышленника с целью обойти алгоритмы классификации [6,7]. Первоначально такого рода воздействия, суть которых обычно заключается в добавлении к входным данным некоторого возмущения (шума), получили распространение в области компьютерного зрения, где глубокие нейронные сети оказались не способны правильно классифицировать изображения по измененным входным данным, и получили название состязательные атаки (adversarial attacks), а подаваемые на вход классификатора данные – состязательные образцы [8]. Подобным образом злоумышленник может атаковать компьютерные сети и обойти СОА на основе глубокого обучения, в результате чего реальная атака может быть классифицирована как нормальная активность и пропущена детектором [9].

Несбалансированность данных при обучении и неустойчивость к состязательным атакам злоумышленников могут негативно влиять на эффективность функционирования СОА на основе машинного обучения, поэтому устранение указанных недостатков является актуальной задачей, требующей решения.

Таким образом, чтобы сбалансировать набор данных и обучить классификатор распознавать состязательные образцы, предлагается применить генеративную состязательную сеть (Generative adversarial network, GAN), модель которой была предложена в 2014 г. Ian’ом Goodfellow’ом и другими экспертами и получила широкое распространение в распознавании изображений [10,11]. GAN – алгоритм машинного обучения, который состоит из генератора и дискриминатора, двух нейронных сетей, имеющих две противоположные цели – создавать образцы и различать образцы.

Материалы и методы

Принцип работы данной модели, архитектура которой представлена на рисунке 1, заключается в обучении генератора G, получающего на вход некоторый шум, имитировать распределение класса атак из обучающего набора данных так, чтобы максимизировать ошибку дискриминатора D, различающего реальные образцы от сгенерированных. В свою очередь, дискриминатор D обучается минимизировать свою ошибку при классификации образцов, которые попеременно подаются на его вход, и вычисляет вероятность того, что входные данные получены из реального набора данных, выдавая на выходе скалярное значение от 0 (сгенерированные) до 1 (реальные). Таким образом, между двумя нейронными сетями возникает состязательная игра, в ходе которой они обучаются.

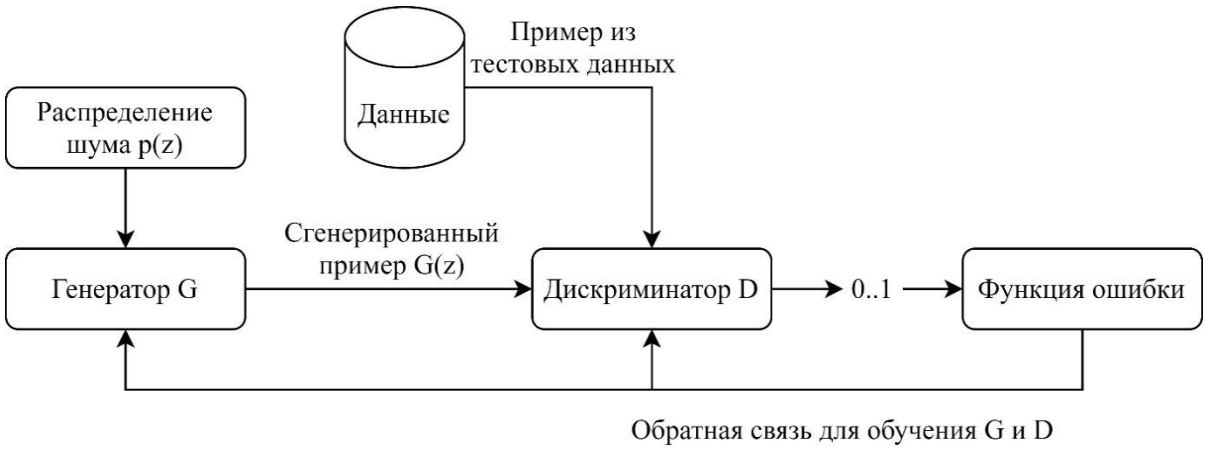

Рисунок 1 – Архитектура генеративной состязательной сети
Figure 1 – Generative adversarial network architecture

Для описания структуры генеративной состязательной модели можно представить генератор G и дискриминатор D как многослойные перцептроны. Определив априорную вероятность шума $p_z(z)$ и представив отображение в пространство данных в виде $G(z;\theta_g)$, где G – это дифференцируемая функция, представленная многослойным перцептроном с параметром θ_g, можно узнать вероятностное распределение генератора p_g над набором данных X.

Также определяется дискриминатор $D(x;\theta_d)$, на выходе которого выводится скалярное значение. D(x) представляет собой вероятность того, что x принадлежит реальному набору данных, а не сгенерированному. При обучении дискриминатора D стоит задача максимизировать вероятность правильного присвоения меток, идентификации как обучающих примеров, так и образцов из генератора G. Вместе с этим при обучении генератора G необходимо минимизировать логарифмическую вероятность $log(\,1 - D(G(z)))$. Таким образом, D и G играют в минимаксную игру для двух игроков [10]:

$$\min_G \max_D V(D,G) = E_{x\sim p_{data}(x)}[log\, D\,(x)] + E_{z\sim p_z(z)}[log(\,1 - D(G(z)))] \quad (1)$$

На каждой итерации обучения, получив из распределений p_g и p_{data} партии из m образцов и вычислив бинарную кросс-энтропийную функцию ошибки (BCE Loss), требуется обновить дискриминатор D в направлении возрастания градиента (2):

$$grad_{\theta_d} \frac{1}{m}\sum_{i=1}^{m}[log\, D\,(x^{(i)}) + log(\,1 - D(G(z^{(i)})))] \quad (2)$$

При это дискриминатор D может обновляться до k раз за одну итерацию, где k – гиперпараметр, подбираемый для лучшего результата обучения. После получения партии из m образцов из распределения p_g и вычисления функции ошибки генератор G обновляется в направлении убывания градиента (3):

$$grad_{\theta_g} \frac{1}{m}\sum_{i=1}^{m} log(\,1 - D(G(z^{(i)}))) \quad (3)$$

Стоит отметить, что при расчёте функции ошибки по формуле (4), где $y^{(i)}$ – целевая метка, когда на вход дискриминатора D подается сгенерированный образец ($y^{(i)} = 0$), вычисляется $log(\,1 - D(G(z^{(i)})))$, а для реального образца ($y^{(i)} = 1$) вычисляется $log\, D\,(x^{(i)})$.

$$L(\theta) = \frac{1}{m}\sum_{i=1}^{m}[y^{(i)}\, log\, D\,(x^{(i)}) + (1 - y^{(i)})\, log(\,1 - D(G(z^{(i)})))] \quad (4)$$

На практике уравнение (1) обеспечивает в начале обучения недостаточный градиент для того, чтобы генератор G хорошо обучался. На ранних этапах обучения, когда генератор G плохо настроен, дискриминатор D может различать сгенерированные образцы с высокой степенью уверенности, потому что они явно отличаются от реальных данных. Вместо обучения генератора G минимизировать вероятность $log(\,1 - D(G(z)))$, необходимо научить его максимизировать вероятность $log\, D\,(G(z))$, что обеспечивает достаточный градиент на ранних итерациях [10].

Процесс обучения генеративных состязательных сетей заключается в обновлении распределения дискриминатора D (синяя пунктирная линия) так, чтобы он мог верно определить принадлежность полученных на вход примеров из распределения обучающего набора данных (черная пунктирная линия) и из распределения сгенерированных образцов (зеленая сплошная линия). Выборка z равномерно составлена из области, представленной на рисунке 2 нижней горизонтальной линией, над которой расположена горизонтальная линия, принадлежащая области x. С помощью стрелок обозначено, как отображение $x = G(z)$ накладывает неравномерное распределение p_g на обучающее. Распределение генератора G сжимается в областях с высокой плотностью, а в областях с низкой – расширяется.

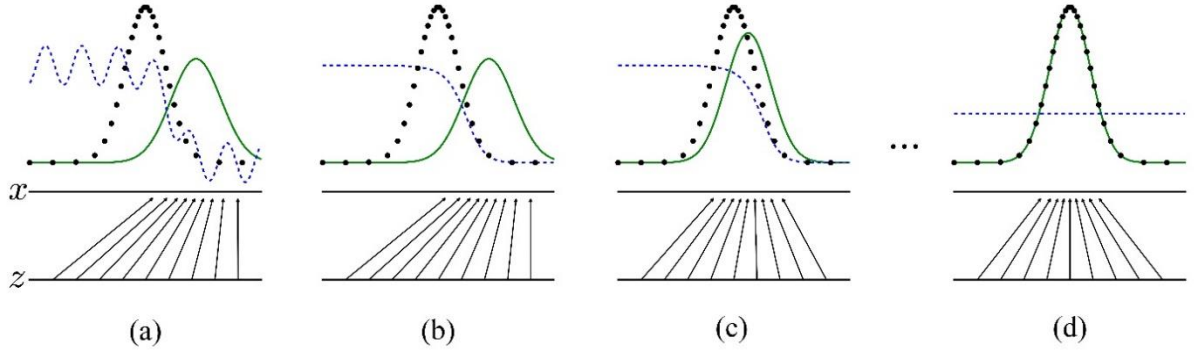

Рисунок 2 – Процесс тренировки генеративной состязательной сети
Figure 2 – The process of training a generative adversarial network

Алгоритм обучения GAN

Отображенный на рисунке 2 процесс имеет следующий алгоритм [10]:

a) Состязательная пара на этапе близкой сходимости: распределения p_g и p_{data} схожи, а *D* является частично-точным классификатором.

b) Внутри цикла *D* обучается различать входные данные, сходясь к $\frac{p_{data}(x)}{p_{data}(x)+p_g(x)}$.

c) Генератор *G* обновляется с помощью градиента *D*, который направляет *G(z)* в область, приближенной к реальным данным.

d) Спустя несколько шагов данный этап становится конечным, *G* и *D* достигают состояния, в котором невозможно дальнейшее улучшение, так как выполняется условие $p_g = p_{data}$, и выход дискриминатора становится равным $D(x) = \frac{1}{2}$.

Описание набора данных NSL-KDD

Для обучения и тестирования предлагается использовать набор данных NSL-KDD, усовершенствованный по сравнению с KDD'99, который состоит из обучающей (training) и тестовой (testing) выборок и является актуальным для применения в СОВ [12]. Строки в наборе данных являются записями сетевого соединения (последовательности TCP, UDP и ICMP-пакетов) и содержат 41 признак, каждый из которых представляет собой определенное свойство или характеристику соединения. Набор данных содержит нормальный трафик и четыре основные категории вредоносного трафика: отказ в обслуживании (DoS, Denial of Service), сканирование для поиска уязвимостей (Probe), получение зарегистрированным пользователем повышенных привилегий (U2R, User to Root) и получение удаленного доступа незарегистрированным пользователем к локальному компьютеру (R2L, Remote to Local). Записи в данном наборе промаркированы: метка «normal» соответствует нормальному сетевому соединению, а иная метка – вредоносному воздействию определенного типа.

Из таблицы 1 видно, что распределение записей по классам неравномерное, набор данных не сбалансирован, из-за чего велика вероятность ошибки при классификации редкого типа атак, поэтому для данного набора целесообразно применение генеративных состязательных сетей.

Таблица 1 – Распределение классов в обучающем и тестовом наборах
Table 1 – Distribution of classes in the training set and test set

Тип набора	Количество записей					
	Всего	Normal	DoS	Probe	U2R	R2L
Train	125973	67343	45927	11656	52	995
		53.46%	36.45%	9.25%	0.04%	0.79%
Test	22543	9711	7458	2421	200	2754
		43.08%	33.08%	10.74%	0.89%	12.22%

В NSL-KDD существует 9 признаков, которые принимают дискретные значения, и 32 признака, имеющие непрерывные значения. В соответствии с описанием каждого признака, можно разделить их, как показано на рисунке 3, на следующие классы: информация о соединении; данные домена; данные, посчитанные в 2-х секундном окне; данные, посчитанные в 100-секундном окне [13].

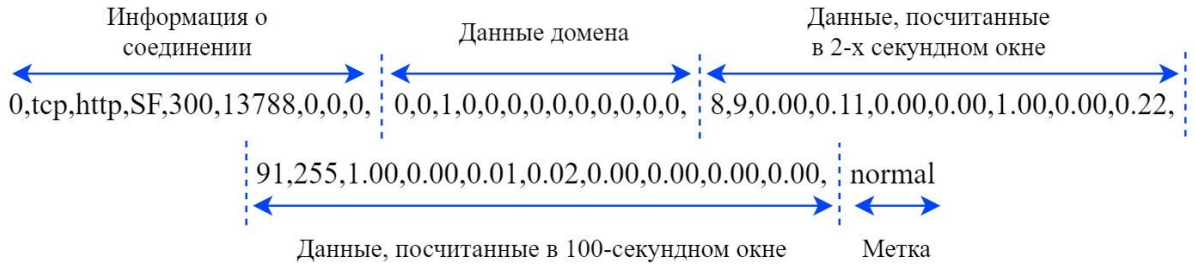

Рисунок 3 – Распределение наборов признаков в строке записи трафика
Figure 3 – The distribution of the feature sets in a line of traffic record

Предварительная обработка данных

Для применения в генеративной состязательной сети требуется предварительная обработка данных из набора NSL-KDD. Необходимо преобразовать символьные значения признаков «protocol type», «service», «flag» в числовые. Например, «protocol type» имеет 3 типа (TCP, UDP и ICMP), которые будут закодированы как 1, 2 и 3. Чтобы исключить негативное влияние неоднородности значений на результаты обучения и тестирования, следует осуществить нормализацию по методу мини-макс (Min-Max) для преобразования данных в интервале [0, 1] в соответствии с формулой:

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}}, \quad (5)$$

где x – значение до нормализации, а x' – значение после нормализации. Кроме того, x_{max} и x_{min} представляют максимальное и минимальное значения признака в наборе данных, соответственно.

Заключение

В данной работе для решения задачи несбалансированности обучающего набора данных и минимизации ошибок при классификации состязательных образцов было предложено использовать генеративные состязательные сети, рассмотрена архитектура модели и алгоритм обучения генератора и дискриминатора. Приведено описание набора данных NSL-KDD, сделан вывод о его несбалансированности из-за малого количества записей в классах U2R и R2L, а также выбран метод нормализации. В дальнейших исследованиях планируется осуществление экспериментальных тестов, в том числе с

проведением сравнительного анализа различных алгоритмов глубоких нейронных сетей при их применении в генеративных состязательных моделях.

БЛАГОДАРНОСТИ

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №19-07-01107\19.

ЛИТЕРАТУРА

1. Scarfone K., Mell P. Guide to intrusion detection and prevention systems. Доступно по: https://csrc.nist.gov/publications/detail/sp/800-94/final DOI:10.6028/NIST.SP.800-94 (дата обращения: 18.10.2020).
2. Бобров А. Системы обнаружения вторжений / Сайт Института механики сплошных сред Российской Академии Наук. Доступно по: http://www2.icmm.ru/~masich/win/lexion/ids/ids.html (дата обращения: 18.10.2020).
3. Явтуховский Е.Ю. Анализ систем обнаружения вторжений на основе интеллектуальных технологий / Технические науки: теория и практика : материалы III Междунар. науч. конф. (г. Чита, апрель 2016 г.). – Чита : Издательство Молодой ученый, 2016. Доступно по: https://moluch.ru/conf/tech/archive/165/10049/ (дата обращения: 18.10.2020).
4. Security Boulevard. Why 2020 will be the year artificial intelligence stops being optional for security. Доступно по: https://securityintelligence.com/articles/why-2020-will-be-the-year-artificial-intelligence-stops-being-optional-for-security (дата обращения: 18.10.2020).
5. Georgios Douzas and Fernando Bao. Effective data generation for imbalanced learning using conditional generative adversarial networks. Expert Systems with Applications. 2018;91;464-471. Доступно по: https://www.researchgate.net/publication/319672232_Effective_data_generation_for_imbalanced_learning_using_Conditional_Generative_Adversarial_Networks DOI: 10.1016/j.eswa.2017.09.030 (дата обращения: 18.10.2020).
6. Security Boulevard. Hacking the hackers: Adversarial AI and how to fight it. Доступно по: https://securityboulevard.com/2020/01/hacking-the-hackers-adversarial-ai-and-how-to-fight-it (дата обращения: 18.10.2020).
7. Weiwei Hu and Ying Tan. Generating adversarial malware examples for black-box attacks based on gan. arXiv preprint arXiv:1702.05983, 2017. Доступно по: https://arxiv.org/abs/1702.05983 (дата обращения: 18.10.2020).
8. Adversarial Attacks in Machine Learning and How to Defend Against Them. Доступно по: https://towardsdatascience.com/adversarial-attacks-in-machine-learning-and-how-to-defend-against-them-a2beed95f49c (дата обращения: 18.10.2020).
9. Zilong Lin, Yong Shi, and Zhi Xue. Idsgan: Generative adversarial networks for attack generation against intrusion detection. arXiv preprint arXiv:1809.02077, 2018. Доступно по: https://arxiv.org/abs/1809.02077 (дата обращения: 18.10.2020).
10. Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley и др. Generative adversarial nets. Advances in Neural Information Processing Systems, 2014. Доступно по: https://arxiv.org/abs/1406.2661 (дата обращения: 18.10.2020).
11. Ming-Yu Liu, Xun Huang, Jiahui Yu, Ting-Chun Wang, Arun Mallya. Generative Adversarial Networks for Image and Video Synthesis: Algorithms and Applications, 2020. Доступно по: https://arxiv.org/abs/2008.02793 (дата обращения: 18.10.2020).
12. Hu L.; Zhang Z.; Tang H.; and Xie, N. An improved intrusion detection framework based on artificial neural networks. In Proceedings of the 11th International Conference on

Natural Computation, 2015. Доступно по: https://www.researchgate.net/publication/304289908_An_improved_intrusion_detection_framework_based_on_Artificial_Neural_Networks DOI: 10.1109/icnc.2015.7378148 (дата обращения: 18.10.2020).
13. Davis J.J., Clark A.J. Data preprocessing for anomaly based network intrusion detection: A review. computers & security, 2011. Доступно по: https://www.researchgate.net/publication/234130888_Post_review_version DOI: 10.1016/j.cose.2011.05.008 (дата обращения: 18.10.2020)

REFERENCES

1. Scarfone K., Mell P. Guide to intrusion detection and prevention systems. Available at: https://csrc.nist.gov/publications/detail/sp/800-94/final DOI:10.6028/NIST.SP.800-94 (accessed 18.10.2020).
2. Bobrov A. Sistemy obnaruzheniya vtorzhenii. Sait Instituta mekhaniki sploshnykh sred Rossiiskoi Akademii Nauk. Available at: http://www2.icmm.ru/~masich/win/lexion/ids/ids.html (In Russ) (accessed 18.10.2020).
3. Yavtukhovskii E.Yu. Analiz sistem obnaruzheniya vtorzhenii na osnove intellektual'nykh tekhnologii. Tekhnicheskie nauki: teoriya i praktika : materialy III Mezhdunar. nauch. konf. (g. Chita, aprel' 2016 g.). Chita : Izdatel'stvo Molodoi uchenyi, 2016. Available at: https://moluch.ru/conf/tech/archive/165/10049/ (In Russ) (accessed 18.10.2020).
4. Security Boulevard. Why 2020 will be the year artificial intelligence stops being optional for security. Доступно по: https://securityintelligence.com/articles/why-2020-will-be-the-year-artificial-intelligence-stops-being-optional-for-security (accessed 18.10.2020).
5. Georgios Douzas and Fernando Bao. Effective data generation for imbalanced learning using conditional generative adversarial networks. Expert Systems with Applications. 2018;91:464-471 Available at: https://www.researchgate.net/publication/319672232_Effective_data_generation_for_imbalanced_learning_using_Conditional_Generative_Adversarial_Networks DOI: 10.1016/j.eswa.2017.09.030 (accessed 18.10.2020).
6. Security Boulevard. Hacking the hackers: Adversarial AI and how to fight it. Available at: https://securityboulevard.com/2020/01/hacking-the-hackers-adversarial-ai-and-how-to-fight-it (дата обращения: 18.10.2020).
7. Weiwei Hu and Ying Tan. Generating adversarial malware examples for black-box attacks based on gan. arXiv preprint arXiv:1702.05983, 2017. Available at: https://arxiv.org/abs/1702.05983 (accessed 18.10.2020).
8. Adversarial Attacks in Machine Learning and How to Defend Against Them. Available at: https://towardsdatascience.com/adversarial-attacks-in-machine-learning-and-how-to-defend-against-them-a2beed95f49c (accessed 18.10.2020).
9. Zilong Lin, Yong Shi, and Zhi Xue. Idsgan: Generative adversarial networks for attack generation against intrusion detection. arXiv preprint arXiv:1809.02077, 2018. Available at: https://arxiv.org/abs/1809.02077 (accessed 18.10.2020).
10. Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley. Generative adversarial nets. Advances in Neural Information Processing Systems, 2014. Available at: https://arxiv.org/abs/1406.2661 (accessed.10.2020).
11. Ming-Yu Liu, Xun Huang, Jiahui Yu, Ting-Chun Wang, Arun Mallya. Generative Adversarial Networks for Image and Video Synthesis: Algorithms and Applications, 2020. Available at: https://arxiv.org/abs/2008.02793 (accessed 18.10.2020).
12. Hu L.; Zhang Z.; Tang H.; and Xie N. An improved intrusion detection framework based on artificial neural networks. In Proceedings of the 11th International Conference on Natural Computation, 2015. Available at: https://www.researchgate.net/publication/

304289908_An_improved_intrusion_detection_framework_based_on_Artificial_Neural_Networks DOI: 10.1109/icnc.2015.7378148 (accessed 18.10.2020).
13. Davis J. J., Clark A. J. Data preprocessing for anomaly based network intrusion detection: A review. computers & security, 2011. Available at: https://www.researchgate.net/publication/234130888_Post_review_version DOI: 10.1016/j.cose.2011.05.008 (accessed 18.10.2020).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Сычугов Алексей Алексеевич, канд. техн. наук, доцент, кафедра информационной безопасности, ФГБОУ ВО «Тульский государственный университет» Институт прикладной математики и компьютерных наук, Тула, Российская Федерация.
e-mail: xru2003@list.ru

Aleksey A. Sychugov, Phd (Tech), information Security Department, Federal State Budgetary Educational Institution of Higher Education «Tula State University», Tula, Russian Federation.

Греков Михаил Михайлович, студент, кафедра информационной безопасности, ФГБОУ ВО «Тульский государственный университет» Институт прикладной математики и компьютерных наук, Тула, Российская Федерация.
e-mail: grekov.web@yandex.ru

Mikhail M. Grekov, Student, Information Security Department, Federal State Budgetary Educational Institution of Higher Education «Tula State University», Tula, Russian Federation.