СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ЛОКАЛНЫХ СЕТЕЙ

Ташметов Т.Ш.,
Ташкентский государственный транспортный университет Ассистент кафедры «Информационные системы и технологии на транспорте», tima260491@gmail.com
Ташметов К.Ш.,
Ташкентский государственный транспортный университет Ассистент кафедры «Информационные системы и технологии на транспорте»,
Гаффаров Н.А.,
Ташкентский государственный транспортный университет Ассистент кафедры «Информационные системы и технологии на транспорте»,
DOI: https://doi.org/10.47689/978-9943-7818-0-1-v2-pp113-117

Аннотация: *Проанализированы возможные последствия несанкционированного доступа к электронной информации. Рассмотрены функции нейронных сетей, позволяющие или в какой-то своей части одной из них, или в их комплексе противодействовать несанкционированному доступу к электронной информации.*

Ключевые слова: *средство защиты, защита информации, несанкционированный доступ; сетевые атаки, хищение информации, утечка информации, DDos атака.*

Введение

Быстрое и повсеместное распространение Интернета привело к бурному развитию компьютерных сетей, что позволило существенно расширить возможности для компаний, предоставляющих свои услуги через глобальную сеть [1]. К глобальной сети подключены миллионы устройств и пользователей, благодаря чему множество фирм и потребителей взаимодействуют между собой [2]. Для реализации своих услуг компании используют информационные ресурсы, которые позволяют выполнять обработку информации, относящуюся к их клиентам [3].

Некорректная работа или недоступность сервисов может повлечь значительные потери, как финансовые информации, так и клиентские информации [4].

Электронная информация, используемая в качестве коммуникатора, навигатора и оператора, внедряется во все сферы деятельности человека [5]. На базе целевых программных продуктов обработки информации и принятия решения осуществляются управление в реальном времени производственно-технологическими, финансово-банковскими, научно-техническими, политическими, энерго-производящими и распределительными, образовательно-просветительными, рекламно-трейдинговыми, стратегически значимыми коммуникационными, военно-оперативными и другими процессами [6]. Поскольку активная экспансия электронной информации происходит во все сферы человеческой деятельности, то уязвимость информации может негативно сказаться на судьбе людей, деструктивно

воздействовать на деятельность предприятий, угрожать экономико-политическим устоям государств и даже перспективам глобальной цивилизации [7].

Несанкционированный доступ к электронной информации может привести к сбою в локальной сети организации; к нарушению каналов связи с внешними партнерами; к уничтожению или блокированию программного обеспечения, числовой, текстовой и графической информации; к хищению паролей, информации со смарткарт; к физическому доступу к плохо охраняемым объектам и к незаблокированным рабочим местам пользователей компьютерной техники, к выведению из строя автоматизированных объектов жизнедеятельности и др. [8].

Именно по этим причинам в последние годы информационные ресурсы и сервисы все чаще сталкиваются с вредоносным воздействием, осуществляемым с использованием протоколов межсетевого взаимодействия – удаленной сетевой атакой.

Среди множества видов сетевых атак наибольшее распространение получила атака типа DDoS. По данным статистики [9, 10] данный вид угрозы занимает одно из лидирующих мест ежегодно. Причинами распространения подобного вредоносного сетевого воздействия является простота реализации, исчерпывающие сведения о механизме исполнения и малые требования к знаниям и вычислительным ресурсам злоумышленника [12, 13].

Взломщика систем защиты информации могут интересовать: государственные информационные ресурсы; конфиденциальные персональные, в т.ч. медико-диагностические и биометрические, данные отдельных частных лиц или всех сотрудников организации и ее клиентов; информация о финансовых ресурсах и потоках; неофициальная переписка; оказываемые физическому лицу сервисные и медицинские услуги; инновационные технологии, инженерно-конструкторские решения, программное обеспечение; еще неопубликованные результаты научно-исследовательских разработок; диагностические методики; используемые формальные и неформальные каналы коммуникаций, транспортно-экспедиционные операции, стратегически значимая инфраструктура [14-15].

Обсуждение

Для предотвращения несанкционированного доступа к хранящейся, обрабатываемой, передаваемой или получаемой информации и, как следствие, для обеспечения безопасности функционирования информационных систем, исключения злонамеренно инициированных сбоев в реализуемых информационно-коммуникационных технологических процессах и пресечения спровоцированной утечки информации применяются системы защиты информации, представляющие комплекс организационно-технологических мер, программно-технических средств, санкционно-правовых и дисциплинарных норм и предписаний.

Регистрируются все более и более изощренные методы посягательства (интервенции) со стороны кибермошенников на серверы компьютерных систем и аккаунты пользователей социальных сетей в целях доступа к особо защищаемой и конфиденциальной информации. С целью хищения

информации путем поиска тех или иных файлов и получения злоумышленником необходимого доступа для их скачивания используются, в частности, сетевые черви, проникающие в компьютерные системы ка через сетевые коммуникационные каналы, так и через съемные носители информации. В первую очередь, уязвимыми с позиций безопасности программного обеспечения и данных являются операционные системы с коммуникационными выходами в интерактивные среды.

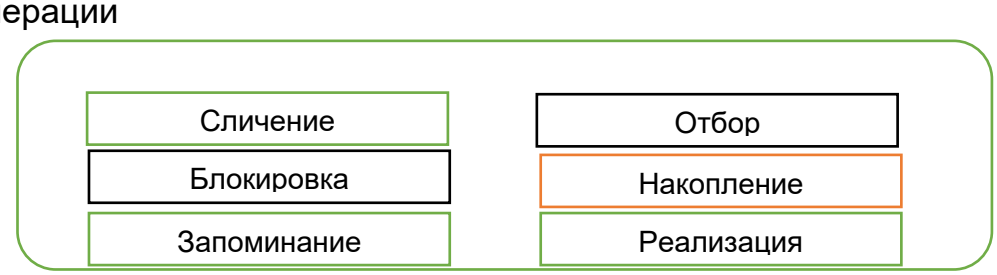
Для успешного противодействия сетевым атакам разрабатываются методы и механизмы защиты; практически все современные программные и программно-аппаратные средства защиты используют целый набор методов. Из-за высокой стоимости средств защиты многие компании отказываются от их приобретения и эксплуатации, что приводит к существенному росту финансовых и клиентских потерь при осуществлении сетевых атак. Основные механизмы, применяемые в современных средствах противодействия DDoS-атакам, представлены в таблице 1 [1].

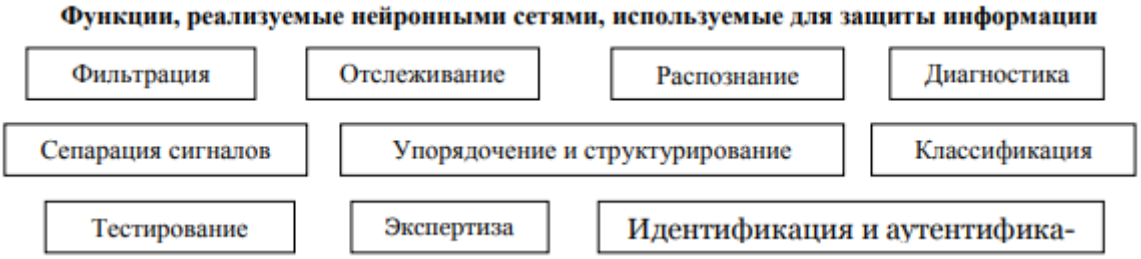
Таблица 1.

Основные механизмы защиты. Сравнительный анализ.

Критерий	**Анализ состояний**	**Нейронные сети**	**Экспертные системы**	**Сигнатурные методы**	**Статистические методы**
Уровень наблюдения	Сеть, ОС, приложение	Сеть, ОС	Сеть, ОС	Сеть, ОС, приложение	Сеть, ОС
Аномалии/ Злоупотребления	-/+	+/+	+/+	-/+	+/-
Верифицируемость	+	-	+	+	-
Адаптивность	-	+	+	-	+
Устойчивость	+	-	+	+	-
Вычислительная сложность	Низкая	Средняя	Высокая	Низкая	Средняя

Одним из наиболее эффективных и перспективных методов обнаружения DDoS-атак является механизм работы нейронных сетей, широко применяющийся в современных средствах защиты. Основные функции, реализуемые нейронными сетями, используемые для защиты информации, представлены в блочной схеме.





Искусственная нейронная сеть – математическая модель, а также её программная или аппаратная реализация, построенная по принципу организации и функционирования биологических нейронных сетей [9-10]. Производительность нейронной сети напрямую зависит от выбранной архитектуры, параметров и метода обучения.

Каждый нейрон представляет собой единицу обработки информации в нейронной сети. В модели нейрона можно выделить три основных элемента [11, 12]:

1. Набор синапсов – входные значения, предаваемые в нейрон. Каждый синапс характеризуется своим весом.
2. Сумматор – складывает значения входных сигналов, взвешенных относительно соответствующих синапсов нейрона.
3. Функция активации – ограничивает амплитуду выходного значения сигнала нейрона.

В модели нейрона также реализован пороговый элемент, который отражает увеличение или уменьшение входного сигнала, подаваемого на функцию активации.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Matvaliyev D., Aliev R. Development of a Program and Algorithm for Determining the Resource of Relays of Automatic and Telemechanics in Railway Transport // Universum: технические науки: электрон. научн. журн. 2022. 11(104).
2. Матвалиев Д., Алиев Р.М. Development of an Algorithm and Program on Mysql to Create a Database to Control the Turnover of Railway Automation Relays // Universum: технические науки: электрон. научн. журн. 2022. 11(104).
3. Алиев Р.М., Алиев М.М., Хакимов Ш.Х., Тохиров Э.Т. Методы расчёта коэффициентов рельсового четырехполюсника бесстыковых рельсовых цепей. Фундаментальная и Прикладная Наука: Состояние и Тенденции Развития: Монография / [Алиев М.М. и др.]. – Петрозаводск: МЦНП «Новая наука», 2022. – С. 537.
4. Tashmetov K.Sh., Aliev R.M., Aliev M.M. Expert system for diagnosing faults railroad switch of automation and telemechanic systems // AIP Conference Proceedings. – AIP Publishing LLC, 2022. – Т. 2432. – №. 1. – С. 030083.
5. Aliev R., Aliev M. Methods calculation for station tonal rail circuits with current receiver // Transportation Research Procedia. – 2022. – Т. 63. – С. 401–411.

6. Aliev R., Aliev M., Tokhirov E. Analysis, development of a model and an algorithm in the concept of the growth of tone jointless rail circuits // Transportation Research Procedia. – 2022. – Т. 63. – С. 178–186.

7. Aliev R., Aliev M. Algorithm for Determining the Optimal Length of the Rail Line by Current Automatic Locomotive Signaling // International Conference TRANSBALTICA: Transportation Science and Technology. – Springer, Cham, 2021. – С. 363–374.

8. Aliev R., Toshmetov K. Telecontrol of the expert system of automatic traffic control // Актуальные вопросы развития инновационно-информационных технологий на транспорте. – 2021. – Т. 2021. – С. 20–22.

9. Кочеткова, 2007 – Кочеткова А.С. (2007). Применение нейронных сетей для мониторинга безопасности информационных сетей // Вестник Волгоградского государственного университета. Серия 9: Исследования молодых ученых, № 6. – С. 163–167.

10. Люгер, 2003 – Люгер Дж.Ф. (2003). Искусственный интеллект: стратегии и методы решения сложных проблем. – М.: Издательский дом «Вильямс». – С. 864.

11. Макарова и др., 2016 – Исследование операций: метод. указания по выполнению расчетно-графических работ. (2016). / сост.: Макарова И.Л., Самарин В.И., Игнатенко А.М. – Сочи: РИЦ ФГБОУ ВО «СГУ». – С. 100.

12. Технологический процесс склада вагонного депо при автоматизации учетных операций. Т.Р. Нурмухамедов, Ж.Н. Гулямов – Sustainable development forum 2022, 2022.

13. Development of the information system for inventory control of wagon depot stock. T.R. Nurmukhamedov, J.N. Gulyamov, T.S. Tashmetov – AIP Conference Proceedings, 2022.

14. Modeling of a railway warehouse commodity and material values accounting (on the example of a train depot). T.R. Nurmukhamedov, Z.N. Gulyamov, S.T. Shaxidaeva – AIP Conference Proceedings, 2021

15. Складские операции вагонного депо пассажирской службы с элементами логистики. Т.Р. Нурмухамедов, Ж.Н. Гулямов – Глобус: технические науки, 2021.