7. *Платонов В.* Программно-аппаратные средства защиты информации: учебник. М.: Academia, 2014. 336 с.
8. *Родичев Ю.А.* Нормативная база и стандарты в области информационной безопасности: учебное пособие. СПб.: Питер, 2017. 256 с.
9. *Семененко В.А.* Информационная безопасность: учебное пособие. 4-е изд., стер. М.: МГИУ, 2010. 277 с.

Literatura

1. *Adamenko M.A.* Osnovy klassicheskoj kriptologii. Sekrety shifrov i kodov. M.: DMK Press, 2012. 256 s.
2. *Biryukov A.A.* Informatsionnaya bezopasnost': zashchita i napadenie. M.: DMK Press, 2012. 474 s.
3. *Gladyshev A.I., Aborkina E.S.* Voprosy primeneniya sushchestvuyushchikh metodov otsenki slozhnosti informatsionnykh sistem // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz, upravlenie". 2016. Vyp. 1–2. S. 114–118.
4. GOST R 51275–2006. Ob"ekt informatizatsii. Faktory, vozdejstvuyushchie na informatsiyu. Obshchie polozheniya. M., 2007. 7 s.
5. Doktrina informatsionnoj bezopasnosti Rossijskoj Federatsii ot 5 dekabrya 2016 g. № Pr-646. M., 2016. 16 s.
6. Informatsionnaya bezopasnost' v korporativnom sektore. URL: http://infowatch.ru (data obrashcheniya: 06.05.2020).
7. *Platonov V.* Programmno-apparatnye sredstva zashchity informatsii: uchebnic. M.: Academia, 2014. 336 s.
8. *Rodichev Yu.A.* Normativnaya baza i standarty v oblasti informatsionnoj bezopasnosti: uchebnoe posobie. SPb. :Piter, 2017. 256 s.
9. *Semenenko V.A.* Informatsionnaya bezopasnost': uchebnoe posobie. 4-e izd., ster. M.: MGIU, 2010. 277 s.

DOI: 10.25586/RNU.V9187.20.02.P.152 УДК 004.052.42+004.056.53

О.Ю. Жарова

РАЗРАБОТКА ИЕРАРХИЧЕСКОЙ МОДЕЛИ ОЦЕНКИ ВНЕШНЕГО ВОЗДЕЙСТВИЯ ДЕСТРУКТИВНЫХ ПОТОКОВ ДАННЫХ НА ТЕХНОЛОГИЧЕСКУЮ СЕТЬ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Цель исследования заключается в разработке инструментария прогнозирования и минимизации возможного ущерба от деструктивных потоков данных, направленных на технологические сети промышленных предприятий. На основе анализа приведены статистические данные, демонстрирующие актуальность проблемы кибератак, направленных на технологические сети промышленных предприятий по всему миру. Описан первый инцидент и последующая динамика нарастания кибердавления. Сделан вывод о причине медленной реакции на инциденты со стороны предприятий. Рассмотрена проблема деструктивных потоков данных в технологических сетях и приведены результаты научно-исследовательской работы, направленной на противодействие им. Приведена и подробно описана разработанная иерархическая модель.

Ключевые слова: технологические сети, киберугроза, DoS/DDoS-атака, внешнее воздействие деструктивных потоков данных, иерархическая модель, статистические параметры трафика.

© Жарова О.Ю., 2020

O.Yu. Zharova

HIERARCHICAL MODEL DEVELOPMENT FOR ESTIMATIO OF DESTRUCTIVE DATA STREAMS EXTERNAL INFLUENCE ON TECHNOLOGICAL NETWORK OF INDUSTRIAL ENTERPRISE

The purpose of this investigation is to develop forecasting tools that can minimize possible damage of destructive data streams targeting technological networks of industrial enterprises. The author cites and analyses statistical data which demonstrate topicality of cyberattacks targeting technological networks of industrial enterprises worldwide. The first incident and subsequent dynamics of cyberpressure increase is described. Author also concludes the reason of slow incident response by enterprises. The problem of destructive data streams in technological networks is considered and results of counteracting scientific research work are shown. Developed hierarchical model is described in detail.
Keywords: technological networks, cyberthreat, DoS/DDoS attack, destructive dataflow external impact, dynamic traffic parameters, hierarchical model, statistical traffic parameters.

Введение

Последние 10 лет технологические сети промышленных предприятий (совокупность технических и программных средств, реализующая оперативную и надежную систему связи с целью передачи служебной информации, контролирования процессов и операций) испытывают постоянно возрастающие кибератаки. До определенного момента киберугрозы были актуальны исключительно для корпоративных сетей. Но после инцидента с червем Stuxnet в 2010 г., атаковавшем SCADA (система диспетчерского контроля и сбора данных) [1; 4; 8; 18], стало ясно, что промышленные предприятия подвержены киберугрозам, при этом риски весьма велики. Атаки на промышленные технологические сети трудоемки и производятся зачастую в несколько этапов. Так, например, предполагаемая первоначальная цель Stuxnet – заводы по производству обогащенного урана – шестая по счету жертва, тогда как первые пять компаний, подвергшихся атаке, работали в сфере разработки промышленных систем или поставки соответствующих комплектующих в Иране. Пятая по счету жертва, помимо продуктов для индустриальной автоматизации, производит центрифуги для обогащения урана. По данным специалистов Лаборатории Касперского, злоумышленники рассчитывали, что компании будут обмениваться данными со своими клиентами – в том числе, с заводами по производству обогащенного урана, тем самым прокладывая путь вредоносным программам к их конечной цели [17; 18]. В тот год было выведено из строя порядка 1000 из 5000 работающих центрифуг IR-1 по обогащению урана, что стало следствием атаки червя Stuxnet [4; 18].

В последние годы создаются все более благоприятные условия для реализации кибератак на промышленные технологические сети, так как происходит активная автоматизация различных технологических процессов промышленных предприятий.

Деструктивные потоки данных в технологических сетях

Специфика и архитектура промышленных и технологических сетей такова, что сложные системы защиты в них неприменимы. Более того, в силу стоимости оборудования

и программного обеспечения для построения технологических сетей, затраты на реализацию защитных модулей промышленными предприятиями зачастую даже не рассматриваются.

В 2017 г. произошел резкий всплеск инцидентов безопасности в области технологических сетей предприятия, и проблема начала принимать глобальные масштабы. Только за первую половину 2017 г. промышленные информационные системы в 63 странах мира подверглись множественным атакам с использованием программ-шифровальщиков [11]. Данная цифра значительно увеличивается, если учесть другие виды атак, среди которых наибольший удельный вес по величине причиняемого ущерба имеет в том числе ***DoS***.

Модернизация производств с уже развернутыми технологическими сетями в современных реалиях сложно осуществима, поэтому даже если риски осознаются руководящим составом, не всегда есть возможность быстро исправить ситуацию и адаптировать существующее оборудование к условиям нарастающего кибердавления извне. Обновление или реконфигурация аппаратно-программных средств АСУ ТП [3; 1] также зачастую влекут за собой большие бюрократические проволочки, и как следствие – реакция на случившиеся инциденты часто запаздывает.

Учитывая все факторы, можно сделать вывод о том, что в ближайшие годы кибердавление на промышленные компании будет только нарастать [10].

Актуальность разработки новых подходов, мер и методов противодействия киберугрозам, перешедшим в разряд угроз технологическим сетям, – не вызывает сомнения. Необходимо учитывать всю специфику узлов и топологий технологических сетей.

В проводимом исследовании основное внимание было уделено DoS- и DDoS-атакам. Как уже упоминалось, данный вид угроз причиняет наибольший ущерб, а так как данные угрозы все еще актуальны и для корпоративных сетей несмотря на большое количество решений разработанных для их предотвращения, то разрабатываемый метод противодействия должен быть универсальным [16].

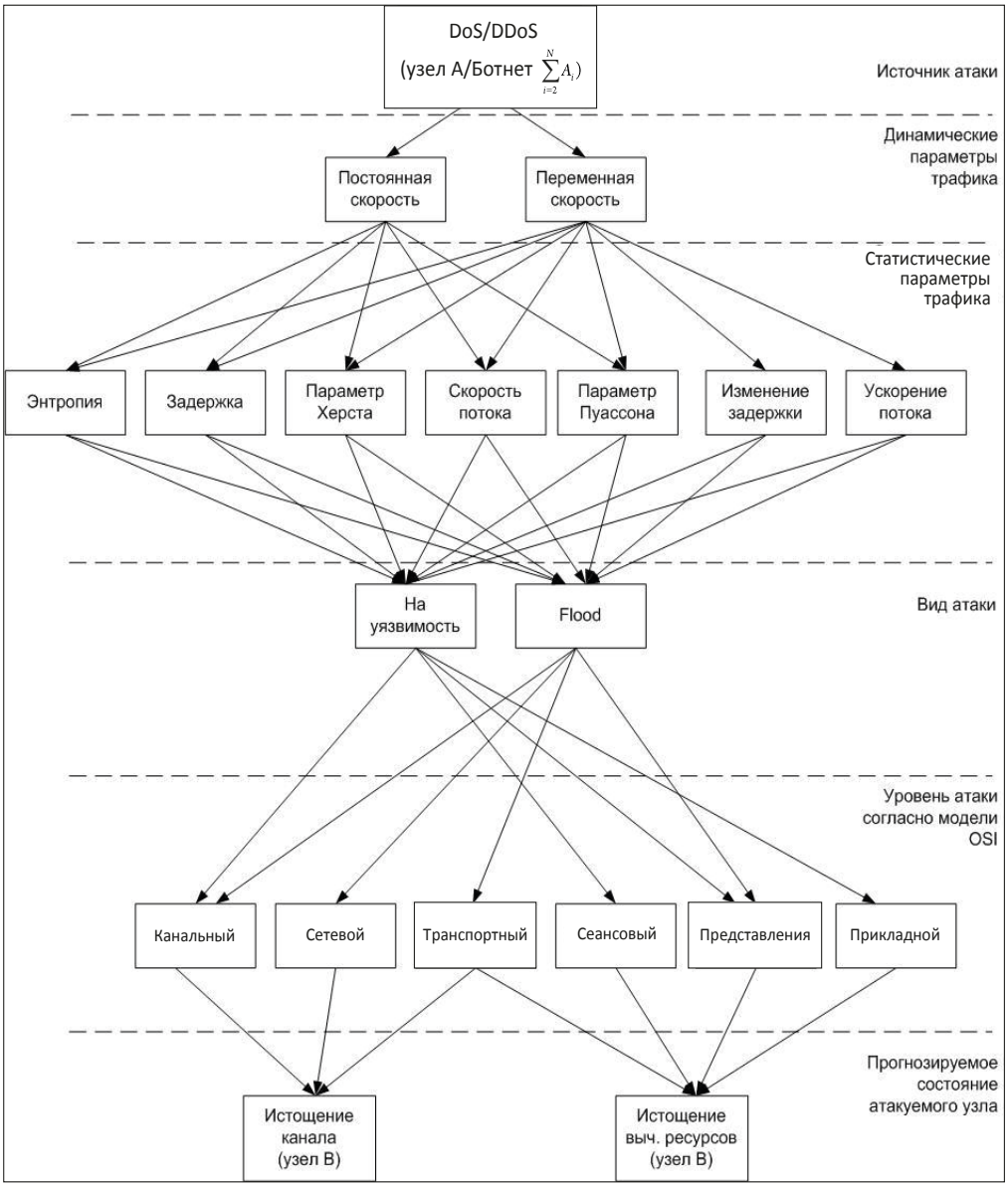
Проблема DoS- или DDoS-атак (Distributed Denial of Service) актуальна для любой распределенной информационно системы. Отличие атак заключается в том, что DoS-атака осуществляется при помощи одного атакующего узла, а DDoS-атака производится при помощи большого числа атакующих узлов (ботнета) [13; 15]. DoS/DDoS-атака – это управляемая интенсификация потоков данных (стремительное повышение числа запросов к атакуемому узлу со стороны атакующего узла/ботнета), приводящая к отказу в обслуживании оборудования, что, в свою очередь, ведет к внеплановому техническому обслуживанию, ремонту или перезагрузке аппаратных средств в составе любой сети, в том числе технологической сети промышленного предприятия [2; 13; 16].

При этом DoS/DDoS-атаки, направленные на технологические сети, это уже не инцидент информационной безопасности, так как не нарушается целостность, конфиденциальность и доступность информационных ресурсов промышленного предприятия. DoS/DDoS-атаки, направленные на технологические сети, – это угроза технологическим процессам, как следствие – снижение эффективности и надежности технологической сети промышленного предприятия [5; 9; 12].

Такого рода атаки всегда таргетированы, часто выполняются с участием инсайдеров.

Иерархическая модель

В рамках проводимой научной работы была разработана и опробована иерархическая модель (рис.). Она имеет 6 уровней и отражает параметры и свойства вредоносного трафика, начиная от момента его генерации источником, заканчивая состоянием атакуемого узла. Это позволяет не только сделать вывод о типе атаки, но и спрогнозировать ее исход, основываясь на параметрах атаки.



Иерархическая модель деструктивных потоков данных

Связи между уровнями сформированы на основе анализа статистических данных по проводимым атакам за период с 1993 по 2019 г., а также исходя из специфики работы каналов передачи данных, в том числе в технологических сетях промышленных предприятий. Набор связей формируют правила осуществления атаки. На каждом уровне, за исключением связей с третьим уровнем, может быть одна связь в зависимости от характера деструктивных потоков данных, при этом модель построена таким образом, чтобы можно было однозначно спрогнозировать исход того или иного вида атаки.

На первом уровне отражен источник атаки, на втором – динамические параметры трафика, зависящие от работы вредоносного программного обеспечения, контролирующего атакующий узел/ботнет. На третьем уровне отражены статистические параметры трафика, позволяющие определить состояние атаки на основе соотношения величин и установленных ранее пороговых значений. Параметров для определения состояния атаки, согласно данной модели, может использоваться от 1 до 7. На основе проведенных исследований были выбраны следующие параметры [7]:

- скорость потока данных;
- ускорение потока;
- пуассоновский поток данных;
- энтропия;
- параметр Херста;
- скорость изменения задержки;
- задержка.

На 4-м и 5-м уровнях рассматривается вид атаки и инструментарий, используемый для организации атаки, соответственно. Под инструментарием в данном контексте понимается сетевой протокол, согласно модели OSI [6, 15], используемый для осуществления атаки. На 6-м уровне рассматривается прогнозируемое состояние атакуемого узла.

Заключение

Анализ потока данных на второй и третьей ступенях иерархической модели с последующим выводом о начале внешнего воздействия деструктивных потоков данных позволяет своевременно принять меры по предотвращению последствий атаки.

Основываясь на динамических и статистических параметрах проходящего в сети трафика, можно сделать заключение о начале воздействия, не дожидаясь полноценной эксплуатации уязвимости или реализации Flood-атаки и не принимая во внимание протоколы обмена данными и их отношение к уровню модели OSI. Своевременные меры позволят избежать перехода атакуемого узла в состояние отказа в обслуживании.

С 4-й по 6-ю ступень производится анализ рисковых событий с прогнозированием состояния узла от успешно реализованной атаки.

Данная модель может применяться для прогнозирования исхода атаки как в технологических, так и в корпоративных сетях.

Литература

1. *Анзимиров Л.В.* SCADA Trace Mode – новые технологии для современных АСУ ТП // Автоматизация в промышленности. 2007. № 4. С. 53–54.
2. *Басканов А.Н.* Способы противодействия и средства раннего выявления DDoS-атак // Экономика и качество систем связи. 2019. № 3 (13). С. 68–76.

3. *Вертешев С.М., Коневцов В.А.* Логическое управление в АСУ ТП // Вестник Псковского государственного университета. Серия «Технические науки». 2015. № 2. С. 93–106.
4. *Головко В.* Кибератаки: вирус-диверсант Stuxnet в ядерной энергетической программе Ирана. Ч. 1 // Наука и техника: Информационные технологии. 2017. URL: https://naukatehnika.com/kiberataki-virus-diversant-stuxnet-v-yadernoj-energeticheskoj-programme-irana-chast1.html (дата обращения: 20.02.2020).
5. ГОСТ 27.002–89. Надежность в технике. Основные понятия. Термины и определения // ТехэкспеRт. URL: http://docs.cntd.ru/document/1200004984 (дата обращения: 25.05.2020).
6. *Давлетшин Р.А.* Сетевой уровень модели OSI. Структура кадра // Современная наука: актуальный вопросы, достижения и инновации: сборник статей IV Международной научно-практической конференции: в 2 ч. Пенза, 2018. С. 45–47.
7. *Жарова О.Ю.* Применение системы анализа сетевой нагрузки для выявления начала DDoS-атаки // Вопросы радиоэлектроники. 2018. № 11. С. 48–52.
8. *Иванов И.А.* SCADA-система XXI века // Автоматизация в промышленности. 2007. № 4. С. 49–51.
9. *Ковалев Д.А.* Классификация методов проведения DDoS-атак // Мир транспорта. 2013. Т. 11, № 1 (45). С. 130–134.
10. Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2018 // Наука и техника. URL: https://naukatehnika.com/kiberataki-virus-diversant-stuxnet-v-yadernoj-energeticheskoj-programme-irana-chast1.html (дата обращения: 20.02.2020).
11. Прогнозы по развитию угроз в сфере промышленной безопасности на 2018 год // Лаборатория Касперского. URL: https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018 (дата обращения: 20.02.2020).
12. *Фролов Д.Ю.* Некоторые аспекты формирования понятия надежности сетей // Мир современной науки. 2011. № 3 (6). С. 18–22.
13. *Хохлов Р.В., Мишин С.А., Солодуха Р.А.* Противодействие DDoS-атакам с помощью анти-DDoS // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2017. № 1. С. 151–156.
14. *Эрнандес Л.* Тестирование на семи уровнях модели OSI // Фотон-экспресс. 2006. № 7 (55). С. 40–42.
15. DoS и DDoS-атаки: значение и различия // DDos-Guard. URL: https://ddos-guard.net/ru/info/blog-detail/dos-i-ddos-ataki-znachenie-i-razlichiya (дата обращения: 20.02.2020).
16. *Hariharan M., Abhishek H.K., Prasad B.G.* DDoS Attack Detection Using C5.0 Machine Learning Algorithm // International Journal of Wireless and Microwave Technologies. 2018. Vol. 9, № 1. P. 52–59.
17. Stuxnet в деталях: «Лаборатория Касперского» публикует подробности атаки на ядерный проект Ирана // Лаборатория Касперского. URL: https://www.kaspersky.ru/about/press-releases/2014_stuxnet-v-detaliakh (дата обращения: 20.02.2020).
18. Stuxnet и ядерное обогащение режима международной информационной безопасности / М.Д. Симоненко // Индекс безопасности. 2013. Т. 19, № 1 (104). С. 233–248.

Literatura

1. *Anzimirov L.V.* SCADA Trace Mode – novye tekhnologii dlya sovremennykh ASU TP // Avtomatizatsiya v promyshlennosti. 2007. № 4. S. 53–54.

2. *Baskanov A.N.* Sposoby protivodejstviya i sredstva rannego vyyavleniya DDoS-atak // Ekonomika i kachestvo sistem svyazi. 2019. № 3 (13). S. 68–76.
3. *Verteshev S.M., Konevtsov V.A.* Logicheskoe upravlenie v ASU TP // Vestnik Pskovskogo gosudarstvennogo universiteta. Seriya "Tekhnicheskie nauki". 2015. № 2. S. 93–106.
4. *Golovko V.* Kiberataki: virus-diversant Stuxnet v yadernoj energeticheskoj programme Irana. Ch. 1 // Nauka i tekhnika : Informatsionnye tekhnologii. 2017. URL: https://naukatehnika.com/kiberataki-virus-diversant-stuxnet-v-yadernoj-energeticheskoj-programme-irana-chast1.html (data obrashcheniya: 20.02.2020).
5. GOST 27.002–89. Nadezhnost' v tekhnike. Osnovnye ponyatiya. Terminy i opredeleniya // TekhekspeRt. URL: http://docs.cntd.ru/document/1200004984 (data obrashcheniya: 25.05.2020).
6. *Davletshin R.A.* Setevoj uroven' modeli OSI. Struktura kadra // Sovremennaya nauka: aktual'nyj voprosy, dostizheniya i innovatsii: sbornik statej IV Mezhdunarodnoj nauchno-prakticheskoj konferencii: v 2 ch. Penza, 2018. S. 45–47.
7. *Zharova O.Yu.* Primenenie sistemy analiza setevoj nagruzki dlya vyyavleniya nachala DDoS-ataki // Voprosy radioelektroniki. 2018. № 11. S. 48–52.
8. *Ivanov I.A.* SCADA-sistema XXI veka // Avtomatizatsiya v promyshlennosti. 2007. № 4. S. 49–51.
9. *Kovalev D.A.* Klassifikatsiya metodov provedeniya DDoS-atak // Mir transporta. 2013. T. 11, № 1 (45). S. 130–134.
10. Landshaft ugroz dlya sistem promyshlennoj avtomatizatsii. Vtoroe polugodie 2018 // Nauka i tekhnika. URL: https://naukatehnika.com/kiberataki-virus-diversant-stuxnet-v-yadernoj-energeticheskoj-programme-irana-chast1.html (data obrashcheniya: 20.02.2020).
11. Prognozy po razvitiyu ugroz v sfere promyshlennoj bezopasnosti na 2018 god // Laboratoriya Kasperskogo. URL: https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018 (data obrashcheniya: 20.02.2020).
12. *Frolov D.Yu.* Nekotorye aspekty formirovaniya ponyatiya nadezhnosti setej // Mir sovremennoj nauki. 2011. № 3 (6). S. 18–22.
13. *Khokhlov R.V., Mishin S.A., Solodukha R.A.* Protivodejstvie DDoS-atakam s pomoshch'yu anti-DDoS // Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologij: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestuplenij. 2017. № 1. S. 151–156.
14. *Ernandes L.* Testirovanie na semi urovnyakh modeli OSI // Foton-ekspress. 2006. № 7 (55). S. 40–42.
15. DoS i DDoS-ataki: znachenie i razlichiya // DDos-Guard. URL: https://ddos-guard.net/ru/info/blog-detail/dos-i-ddos-ataki-znachenie-i-razlichiya (data obrashcheniya: 20.02.2020).
16. *Hariharan M., Abhishek H.K., Prasad B.G.* DDoS Attack Detection Using C5.0 Machine Learning Algorithm // International Journal of Wireless and Microwave Technologies. 2018. Vol. 9, № 1. P. 52–59.
17. Stuxnet v detalyakh: "Laboratoriya Kasperskogo" publikuet podrobnosti ataki na yadernyj proekt Irana // Laboratoriya Kasperskogo. URL: https://www.kaspersky.ru/about/press-releases/2014_stuxnet-v-detaliakh (data obrashcheniya: 20.02.2020).
18. Stuxnet i yadernoe obogashchenie rezhima mezhdunarodnoj informatsionnoj bezopasnosti / M.D. Simonenko // Indeks bezopasnosti. 2013. T. 19, № 1 (104). S. 233–248.