АНАЛИЗ МЕТОДОВ И СРЕДСТВ ОБНАРУЖЕНИЯ КИБЕРУГРОЗ В БОЛЬШИХ ДАННЫХ

Гуломов Шерзод Ражабоевич
(ТУИТ, доцент Зав.кафедрой ИБ)

Мамаев Нурат Наримонович
(ТУИТ, магистрант ИБ)

Аннатация: Развитие информационных и коммуникационных технологий передачи и обработки информации влияет даже на лексический состав и орфографические правила многих языков мира. как анализ механизмов нарушения защиты киберпространства, моделирование разрушающих воздействий; управление кибербезопасностью, определение зоны устойчивости объекта защиты, анализ киберрисков, разработка стандартов и нормативов безопасности киберпространства; синтез средств защиты киберпространства и контроль текущего состояния и функционирования компонентов киберпространства. Кибербезопасность объединяет подходы, методы и средства защиты киберфизических систем больших данных. Основными компонентами модуля являются: блок мониторинга на базе технологий больших данных; блок инвариантной к угрозам оценки самоподобия системы и прогнозирования; блок выработки решения и блок управления.

Ключвой слова: киберпространство, кибербезопасность, киберпреступность, кибертерроризм, кибератака, кибервойска, кибероружие, большие данные.

Ведение:
Изменения современного мира, вызванные бурны ростом с информационных технологий и всеобщей цифровизацией, не могли не затронуть производственные системы. Изобретение и повсеместное использование программируемых контроллеров, роботов и цифровых систем управления, интегрированных с корпоративными сетями предприятий, привело к изменению подходов к управлению производством, бурному развитию нескольких новых технологических управлений(1-3). Ускоренное развитие информационных технологий за последние 30 лет значительно изменило мир в самых различных сферах. Глобальная информатизация общества является одной из доминирующих тенденций развития человеческой цивилизации в XXI в. Стремительное развитие информационных технологий, увеличение возможностей телекоммуникационных систем приводит к появлению новых вызовов и угроз, совершаемых в киберпространстве.

Средств кибербезопасность:
Развитие информационных и коммуникационных технологий передачи и обработки информации влияет даже на лексический состав и орфографические правила многих языков мира. Стали появляться и все чаще использоваться слова-неологизмы с приставкой «кибер-» (англ. cyber-): киберпространство, кибербезопасность, киберпреступность, кибертерроризм, кибератака, кибервойска, кибероружие, киберсотрудничество и т.д (4-5).
Кибербезопасность — это набор принципов и средств обеспечения безопасности информационных процессов, подходов к управлению безопасностью и прочих технологий, которые используются для активного противодействия реализации киберугроз. Задачи обеспечения кибербезопасности могут быть систематизированы как анализ механизмов нарушения защиты киберпространства, моделирование разрушающих воздействий; управление кибербезопасностью, определение зоны устойчивости объекта защиты, анализ киберрисков, разработка стандартов и нормативов безопасности киберпространства; синтез средств защиты киберпространства и контроль текущего состояния и функционирования компонентов киберпространства(6-9). В соответствии с этим современная парадигма обеспечения безопасности включает:

1. Пересмотр моделей управления доступом, учитывающих открытость, гибкость и распределенность. Модели должны быть основаны на темпоральной логике.
2. Принятие технологии виртуализации как мощнейшего средства защиты, которое позволяет перейти от понятия «защищенной системы» (от фиксированного множества угроз) к понятию «система с прогнозируемым поведением».
3. Реализация принципа разделения среды обработки информации и средств защиты.
4. Построение теоретических основ управления динамической защитой (адаптирующейся к текущим угрозам) как объекта автоматического регулирования с понятием зоны устойчивости, последействием (инерционностью) динамическими характеристиками
5. Принятие открытости систем (связь с Интернет) как неотъемлемого свойства и построение защиты с учетом этого:
6. Разработка основ оценки эластичности (настраиваемости системы) и масштабируемости. Разработка новых принципов обнаружения атак, вирусов, руткитов, червей, РПС и прочего ВПО.
7. Учет возможности использования суперкомпьютеров для создания новых сценариев атак, систем сканирования, вмешательства в управление производством, криптоанализа. Учитывая, что мы вошли в эпоху кибервойн, суперкомпьютер - возможность создания нового оружия.
8. Анализ существующих тенденций развития средств обеспечения безопасности позволяет сделать вывод о смене парадигм защиты, базирующихся на технологиях защиты, которые условно могут быть определены как статическая, активная, адаптивная и динамическая. Идея такой классификации технологий защиты заимствована из теории управления.

Несмотря на различие целей, преследуемых в теории управления и теории защиты информации, можно увидеть сходство подходов, используемых для достижения этих целей и направленных на удержание системы в границах некоторого набора состояний(10-14).

Облачными технология:

Составляющие части цифровая инфраструктуры могут быть разделены на следующие группы, согласно соответствующим им современным информационным технологиям:

Квантовые технологии;
Технологии искусственного интеллекта;
Облачные технологии;
Технологии больших данных;
Технологии киберфизических систем.

Под облачными технологиями, как правило, понимается предоставление пользователю компьютерных ресурсов и мощностей в виде интернет-сервисов. При это, пользователь может не иметь информации о том, какие вычислительные машины обрабатывают его запросы, какая при этом используется операционная система. Вычислительные облака состоят из тысяч серверов, размещенных в центрах обработки данных. Они единовременно обеспечивают миллионы пользователей необходимыми вычислительными мощностями.

Учитывая, что облачные технологии, как правило, используются для хранения, передачи данных, а также или выполнения вычислительных задач, они значительно расширяют спектр киберугроз информационно й инфраструктуры, особенно в части конфиденциальности информации и доступности информационных ресурсов.

Общепринятой терминологии в области обработки больших данных еще не сложилось. Однако, термину «большие данные» можно дать следующее определение - это массивы данных такого объема и структуры, которые превышают возможности традиционных программных инструментов по сбору, хранению и обработке данных за приемлемое время При этом данные могут быть структурированными, слабоструктурированными и неструктурированными, что не позволяет эффективно управлять ими и обрабатывать традиционным образом(15).

Киберугроз в больших данных:

Проблема обеспечения безопасности больших данных заключается в противоречии между возрастающими потребностями в обработке таких данных с одной стороны, и недостаточными

возможностями гарантировать конфиденциальность, целостность, доступность обрабатываемых данных и компонентов инфраструктуры с другой. Проблемы обеспечения кибербезопасности вызывают необходимость выработки принципиально иных подходов, базирующихся на концепции защиты распределенной, крупномасштабной вычислительной среды больших данных, а не единой физической сущности(16).

В первой половине 2020 года, по материалам специального отчета «Cyberwar and the Future of Cybersecurity», опубликованного Tech Republic, номером один являются внешние вредоносные источники, затем идут случайные инциденты и вредоносные инсайдеры (рис. 1). Таким образом, от года к году первая тройка источников кибератак не изменяется и данные источники можно признать «традиционными».

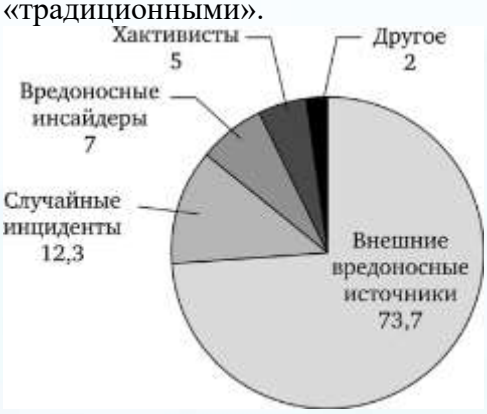

Рис. 1. Распределение ответственности за кибератаки в 2020 г., %

Среди основных причин и проблем, являющихся источниками кибератак, называются разнообразные уязвимости (21 %), злонамеренная активность (19 %) и вредоносные программы (14 %) .(табл. 1).

Таблица 12

Проблемы, вызывающие наибольшую озабоченность в разных странах, %

Наименование	2020	США	Велико британия	Канада	Австра лия	Син гапур
Обнаружение уязвимостей	21	22	19	32	24	25
Обнаружение вредной активности	22	23	20	19	15	23
Обнаружение вредоносного ПО	15	13	18	25	19	18
Предотвращение социального инжиниринга / фишинга	15	13	16	18	12	19
Усиление паролей и удаленный доступ	12	12	13	6	15	11
Управление сетями, устройствами и удаленными пользователями	10	11	12	8	11	6
Патчинг уязвимостей	8	8	10	8	11	6
Обработка инцидентов	4	4	5	3	3	5

В материалах отчета также можно обнаружить основные критические технологии с точки зрения давления на ИТ-специалистов и имманентного риска (табл. 2). Как и в прошлые годы, новые технологии вынуждают ИТ-специалистов развертывать решения в «облаках», на втором месте 1оТ-технологии, затем BYOD. Все больше компаний полагаются на личные устройства сотрудников (смартфоны, планшеты и др.), поэтому ИТ-специалистам приходится внедрять и развертывать BYOD-решения. Безопасность и комфорт облачных технологий в 2020 году возросли, в результате число

респондентов, которые рассматривали облака как технологию, создающую наибольшие риски, снизилось с 45 % в прошлом году до 38 % в отчете этого года.

Таблица 2

Критические технологии сточки зрения рисков безопасности, %

Технологии	2018	2020	США	Велико британия	Австра лия
Облачные технологии	42	40	38	37	36
Интернет вещей (IoT)	—	22	23	20	30
Использование личных устройств (BYOD)	30	22	23	27	18
Социальные медиа	13	15	14	12	22
Мобильные приложения	14	10	11	9	4
Большие данные	7	6	8	9	3

Заключение

В статье предложена анализ методов и средств обнаружения киберугроз в больших данных, особенности в больших данных, с точки зрения технологических изменений и изменений в области защищенности. Приведены основные технологии, легшие в основу индустриальных изменений и их влияние на производство и технологии защиты информации. больших данных производства, появление киберфизических объектов и систем, формирование киберсреды, является неизбежным следствием повсеместного использования программируемых контроллеров и компьютеризации процессов управления. Одновременно наблюдается рост и изменение специфики атак на производственные системы. В этих условиях важным направлением становится развитие кибербезопасности, как части информационной безопасности. Кибербезопасность объединяет подходы, методы и средства защиты киберфизических систем больших данных. Основными компонентами модуля являются: блок мониторинга на базе технологий больших данных; блок инвариантной к угрозам оценки самоподобия системы и прогнозирования; блок выработки решения и блок управления. Успешное внедрение решений безопасности обеспечивается применением управлении технологическим процессом.

Литература:

1. Фабиано Валлеси. Цифровая атака. URL: http://pbwm.ru/articles/ tsifrovaya-ataka (дата обращения: 23.11.2015). 93
2. Jon Oltsik, Analytics-based approach to cyber security. May, 2015. URL: https://www. splunk.com/content/dam/splunk2/pdfs/white-papers/esg-solution-showcase-splunk-may-2015.pdf. (дата обращения: 23.11.2015).
3. Reuters: Российские хакеры похитили личные данные 272 млн. пользователей. URL: https://aftershock.news/?q=node/395028. (дата обращения: 04.05.2016).
4. Research: Thwarting sophisticated cyberattacks demand better grasp of big data with more proactive analytics. SAS Global Forum, Dallas, Apr. 27. 2015.
5. K. Khujamatov,T.Toshtemirov Wireless sensor networks based Agriculture 4.0: challenges and apportions 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan – 2020.-5 p
6. Сбербанк оценил потери экономики от кибератак в 600 миллиардов рублей. URL: https://lenta.ru/news/2016/06/10/cyberattack/.(дата обращения: 10.06.2016).
7. McAfee. An Intel Company. Экономические последствия киберпреступности и кибершпионажа. Центр стратегических и международных исследований (CSIS): отчет. 2013.
8. Big Data and Predictive analytic: on the cyber security front line. IDC white paper, February, 2015, IDC #254290.

9. RX Djuraev, SY Djabbarov, TQ Toshtemirov Analysis of the relationship between the indicators of controllability and reliability characteristics of data transmission systems 2019 International Conference on Information Science and Communications.

10. The Global Risks Report 2016 11th Edition. – World Economic Forum. URL: http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf. (дата обращения: 10.06.2016).
11. Доктрина информационной безопасности Российской Федерации: проект. Совет Безопасности Рос. Федерации. URL: http://www.scrf.gov.ru/ documents/6/135.html. (дата обращения: 10.06.2016).
12. Кибервойна только набирает обороты – НАТО вступает в игру. InfoResist. URL: https://inforesist.org/kibervoyna-tolko-nabiraet-oborotyi-nato-vstupaet-v-igru/ (дата обращения: 09.07.2016)
13. **Halimjon Khujamatov,, Temur Toshtemirov , Doston Turayevich Khasanov, Nasiba Saburova, Ilhom Ikromovich Xamroyev** IoT based agriculture 4.0: challenges and opportunities Bulletin of TUIT: Management and Communication Technologies
14. Kh E Khujamatov, TK Toshtemirov, AP Lazarev, QT Raximjonov IoT and 5G technology in agriculture 2021 International Conference on Information Science and Communications Technologies (ICISCT)
15. 15.Temirova Dilfuza Xusanovna, Kadirova Laylo Imomaliyevna, Fayzullayeva Barno Baxadirovna SENSOR NETWORKS AND THEIR DEVELOPMENT ALGORITHM . Journal of Critical Reviews.
16. Salimjon Mahmudov Dilfuza Temirova . Load Balancing Method in Smart City Networks based Software Defined Networking .