Разработка методики анализа устойчивости объектов ЗОКИИ к компьютерным атакам путем моделирования с использованием концепции сетей Петри

Любименко Дмитрий Анатольевич
Заместитель генерального директора АО «ПО «Аквамаш», г. Волгоград, Россия, d.lyubimenko@aquamash.ru
Аспирант Волгоградского государственного технического университета

АННОТАЦИЯ

Введение: разработка методологии анализа устойчивости значимых объектов критической информационной инфраструктуры к взлому, компьютерным атакам, воздействию вредоносных компьютерных программ. **Цель исследования:** используя концепцию построения сетей Петри, гиперсетей выполнить моделирование объектов значимой критической информационной инфраструктуры. **Результаты**: предложенная методика построения модели объектов ЗОКИИ позволит точно определить показатели вероятности компьютерной атаки, разработать схему устойчивости к не легитимному воздействию. Разрабатываемый метод построения модели учитывает специфику объектов ЗОКИИ: особенности коммуникации, построения корпоративной сети передачи данных (КСПД), динамику эксплуатации. Все перечисленные факторы влияют на устойчивость системы к взлому. Решается задача оценки защиты, обеспечения информационной безопасности ЗОКИИ. Методика позволяет снизить зависимость от субъективных экспертных оценок, закрывает вопрос соблюдения требований законодательства в части выполнения требований Федеральной службы по техническому и экспортному контролю. Ежегодное ужесточение правил эксплуатации объектов критической инфраструктуры требует особого подхода. Эксплуатация методики представляет собой организационную меру защиты от проникновения злоумышленников. **Практическая значимость**: возможность с высокой точностью моделировать параметрические модели объектов критической информационной инфраструктуры. При моделировании учитываются оценки защищенности коммуникационных, инфраструктурных параметров самого объекта. Кратно повышается независимость оценки состояния информационной безопасности корпоративных сетей передачи данных, объектов ЗОКИИ других типов (АСУ, АСУ ТП) субъектов, работающих в оборонной промышленности. Что особенно актуально перед плановыми и внеплановыми проверками со стороны регуляторов (ФСТЭК, ФСБ). Следование методики снижает вероятность назначения штрафов руководителю предприятия, специалисту по информационной безопасности.

КЛЮЧЕВЫЕ СЛОВА: защита информации, ЗОКИИ, КИИ, математическое моделирование, устойчивость

Введение

Вопрос обеспечения информационной безопасности для информационно-телекоммуникационных сетей (ИТС), автоматизированных сетей управления (АСУ) используемых для решения задач в вычислительных системах на субъектах КИИ особенно остро стоит на оборонных предприятиях. Нацелены злоумышленники на объекты ЗОКИИ. Проникновение внутрь защищенного периметра, получение повышенных привилегий становится причиной серьезного экономического, репутационного ущерба для предприятия [1].

В рассматриваемом примере в качестве объектов КИИ могут выступать станки с числовым программным управлением (ЧПУ), корпоративная сеть передачи данных (КСПД). Схема настройки работы. При построении инфраструктуры используются типовые решения: VPN-каналы для защиты передаваемых данных, резервирование, построение системы защиты периметра, отказоустойчивость при атаках злоумышленников (DDos, других). В перечисленных условиях решить проблему защищенности на субъектах КИИ возможно с помощью оборудования отечественного производства. Требование предъявляется нормативной документацией, разработанной ФСТЭК, ФСБ России [15]. Перечень оборудования, поддерживаемых система определяется категорией объекта КИИ присвоенного в соответствии с нормативной документацией [3].

Основными компонентами КИИ, эксплуатируемых на субъектах, относящихся к оборонной промышленности, являются: ЦОД (центры обработки данных), КСПД либо её фрагмент, АСУТП. Примерная схема распределенной информационной транспортной сети оборонного предприятия, эксплуатирующего ЗОКИИ, приведен на рис. 1. Она представлена иерархической структурой, построена на межсетевых экранах нового поколения (NGFW), имеющих сертификат ФСТЭК [20].

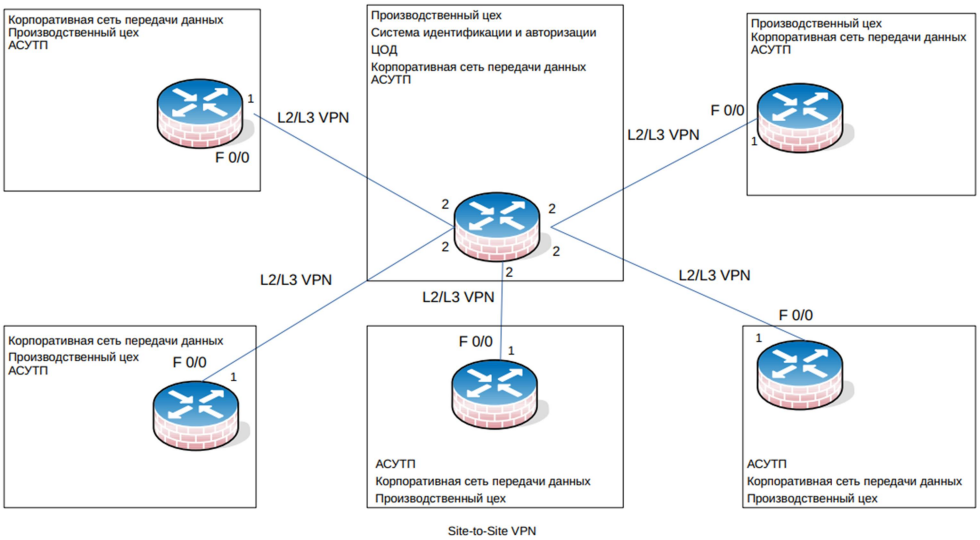

Рис. 1 Корпоративная сеть передачи данных для объектов КИИ (АСУТП, ИТС)

В 2024 году был сформирован перечень типовых объектов КИИ для оборонной промышленности. Полный перечень включает в себя 42 позиции. Существует несколько подходов к проектированию, реализации защищенной сети передачи данных. Выделяют несколько основных требований: использование VPN с шифрованием трафика (на субъектах КИИ – VPN ГОСТ), резервирование оборудования и канала связи. Особый критерий – устойчивость к компьютерным атакам (КА) [19]. Особые требования предъявляются к коммутационным программно-аппаратным комплексом. Средства межсетевого экранирования, используемые для построения VPN и системы защиты периметра (СЗП), должны соответствовать требованиям ФСТЭК и иметь соответствующий сертификат. Законодательство не определяет требования к объектам критической информационной инфраструктуры без категории. Но практика контактов с федеральной службой технического и экспортного контроля указывает на необходимость использования сертифицированных средств защиты [17]. Остальное оборудование для сетевой коммутации, не являющееся частью СЗП, должно быть обязательно российского производства.

Опасность для КСПД представляют нарушители внутренние и внешние. Воздействовать злоумышленник на сеть передачи данных может разными способами. Уязвимость обуславливается

концепцией инфраструктуры, особенностями организации каналов передачи данных. Наиболее уязвимое звено в многоуровневой сети передачи данных – сеть провайдера, выступающая в качестве опорной. Существует несколько способов защиты каналов передачи данных: технические и организационные. Под последними подразумевается соглашение о неразглашении [2]. Техническая защита каналов связи требует разделения сети на уровни (сеть оператора связи/одноранговая/оверлейная). На рисунке 2 представлена схема взаимодействия отдельных узлов.

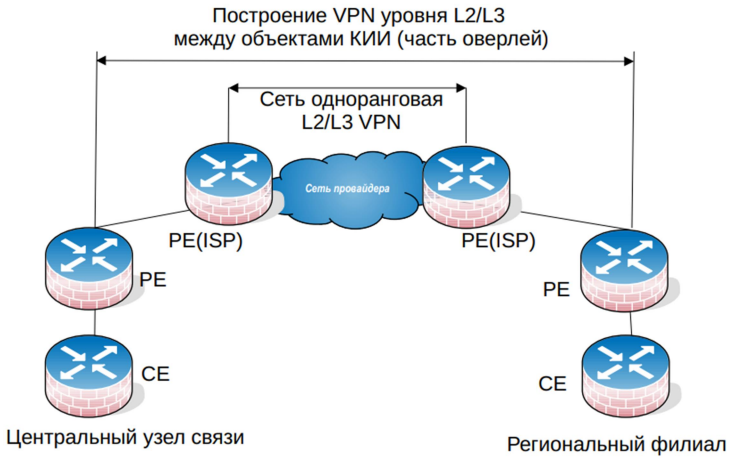

Рис. 2 Классическая схема работы распределенной сети передачи данных предприятия ОПК

Разработан ряд параметров, характеризующих объекты КИИ по степени защищенности (целостность, доступность, конфиденциальность данных). Техническая возможность отражать КА – основное свойство объекта, относящегося к категории критических [5].

Вопрос устойчивости работы КИИ определяется возможности противостоять компьютерным атакам. Такая задача может решаться за счет отказоустойчивости достигаемой резервированием. Критерии определяются рисками вероятностного характера, методом построения Марковских цепей. В работе предлагаю применять два основных метода оценки киберустойчивости (теории): риски, вероятности, множества. Нарушители действуют нелинейно. Квалификация специалистов, занимающихся взломом, с каждым годом возрастает [7]. При проектировании системы защиты периметра обязательно учитываются два критерия – киберустойчивость и защищенность. Перед началом проектирования СЗП проводится обследование, рассчитываются оценки защищенности объекта, определяются параметры защищенности, методов воздействия нарушителя. Следующий этап построения системы защиты периметра – определение параметрических особенностей. Выбираются методы противодействия КА. Практические исследования, проведенные в реальных условиях компьютерных атак разного типа, подтверждают эффективность защиты каналов связи путем динамического изменения параметров работы [16]. Такой подход к обеспечению системы защиты соответствует критериям функционального обеспечения устойчивости. Способ резервирования определяется техническими возможностями. Это могут быть настройки логического канала передачи данных, характеристики используемых виртуальных сетей (VPN), настройка маршрутизации трафика внутри КСПД и QoS (рис. 3).

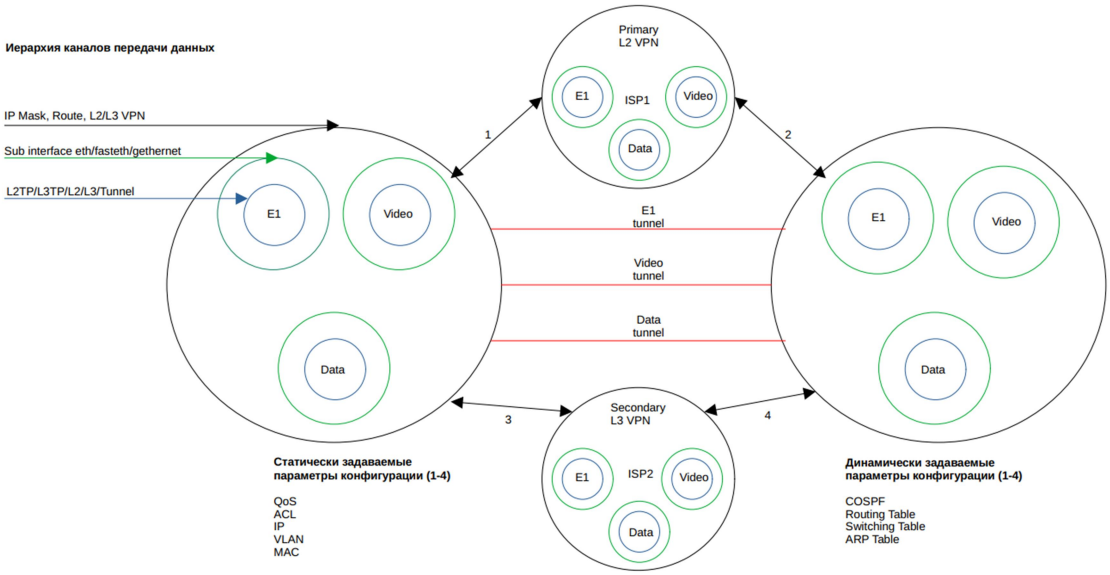

Рис. 3 Модель вложенной структуры КСПД предприятия

Выбор технологии создания туннелей на уровнях L2/L3 VPN на субъектах критической информационной инфраструктуры всегда ограничивается государственным стандартом. При проектировании системы с требованиями к отказоустойчивости предполагается использование как физического, так и логического резервирования каналов (используются протоколы RSTP, VRRP) [6].

Построение логических каналов подразумевает наличие определенной иерархии. Она строится на параметрах конфигурации объектов, работающих внутри сетевого периметра. Процесс проектирования и исследования уже существующих объектов КИИ предполагает использование математических методов моделирования [3]. В работе используется теория гиперграфов. Применяемый подход будет учитывать особенности иерархии построения (построенной) КСПД, физические связи.

Моделирование и анализ связей значимых объектов критической информационной инфраструктуры

Анализу, проектированию моделей устойчивости объектов КИИ посвящено множество работ. Но они не учитывают параметрические особенности моделирования протоколов. Построение математической модели с использованием графов позволит полностью отразить параметры объекта КИИ. Удобно использование гиперграфов – с их помощью можно с высокой точностью определить с учетом вероятности возникновения угрозы. При моделировании таким способом учитываются факторы: способ передачи трафика, конфигурация оборудования и его тип, вероятность возникновения конфликтов в процессе работы [4].

Для выполнения процедуры математического моделирования используется теория s-гиперсетей. Она позволяет в процессе построения моделей учитывать одновременно несколько элементов: инфраструктурные, конфигурационные, иерархические. Математическое выражение теории представлено в выражении №1 [3].

$$H = (G_f, G_1, \dots, G_m, G_п, G_H), \qquad (1)$$

– где G_f – граф физической топологии;
– $G_{1,m}$ – граф инфраструктурных компонентов;
– $G_п$ – гиперграф политик ИБ;
– G_v – гиперграф воздействия нарушителя;
– G_H – гиперграф воздействия нарушителя.

Рассмотрены основные теории, представленные в работах s-гиперсетей и подходы к математическому моделированию. Можно сделать вывод о наличии ограничений, обусловленных сложностью выбранных объектов, сформированных в матрицу инцидентности, необходимостью изменения графа и приведения к необходимому виду. Перечисленные сложности возможно

устранить с помощью функционала сетей Петри (используются раскрашенные вложения). Они позволяют воспроизвести работу защищенных объектов критической информационной инфраструктуры, получить точный результат и проанализировать его [18]. Изменение динамики гиперграфа, используемого для моделирования – следствие воздействия злоумышленника (внешнего или внутреннего). Воздействия различного рода. Например, внесение изменений в конфигурацию, коммуникационную составляющую ЗОКИИ. Все модели, используемые для имитации работы в схеме гиперграфов, представлены в выражении 2.

$$S = (\{R_д, R_{иб}, R_v\}, \{F_д, F_{иб}, F_v\}, \{J_д, J_{иб}, J_v\}, N_0\}) \quad (2)$$

- где $R_д$ – максимальная величина допустимых значений ЗОКИИ;
- $R_{иб}$ – максимальная величина позиций политик ИБ;
- R_v – максимальное количество воздействий нарушителя;
- $F_д$ – максимальное количество допустимых переходов;
- $F_{иб}$ – максимальное множество переходов политик ИБ;
- F_v - максимальное множество воздействий нарушителя;
- $J_д$ – максимальное множество дуг допустимых переходов,
- $J_{иб}$ – допустимое множество дуг событий политик;
- J_v – максимальное множество дуг событий воздействия нарушителей;
- N_0 – начальное состояние сети.

Принцип моделирования объектов методом гиперсетей представлен на рисунках 4-8. Работу объектов критической информационной инфраструктуры формирует стек протоколов разных уровней OSI (Eth, VLAN, ARP, RSTP, IP, ICMP, L2VPN) [10]. Протоколы задействуются внутри периметра и за его пределами – на базе опорной сети провайдера. Вложенность протоколов представлена на рисунке №4.

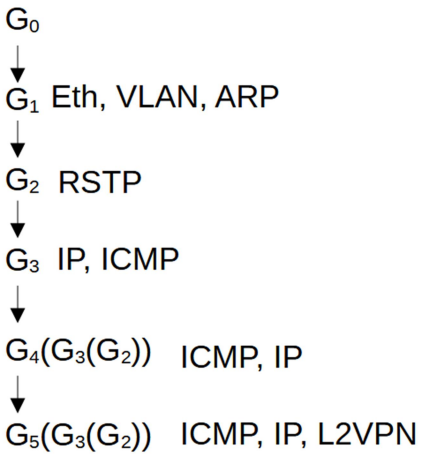

Рис. 4 Вложения графов в гиперсети S

Граф на рисунке 4 отображает идеологию сети передачи данных используемую для связи между отдельными объектами критической инфраструктуры. Ребра графов второго, третьего, четвертого и последующих уровней определяются ребрами. Все они участвуют в работе протоколов различных уровней [9]. Рисунок №4 описывает стандартную топологию – G0. Первые три номера (1, 2, 3) – это конечные объекты (АСУ, АСУ ТП). Номера с четвертого по шестой - коммутационное оборудование, работающее на уровне L2. Номера седьмой и восьмой – маршрутизаторы (роутеры, работающие на уровне L3). В схеме присутствует также оборудование поставщика связи – провайдера. Маркируется номеров девять и десять, работает на уровне L2, L3.

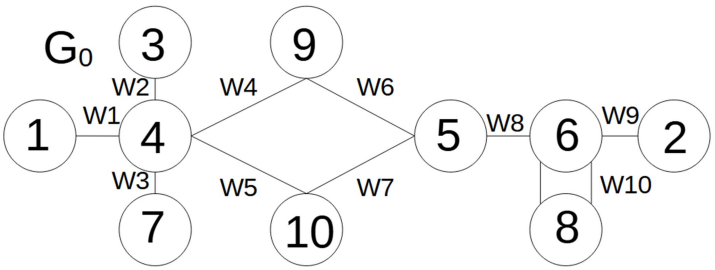

Рис.5 Граф первичного типа для информационной транспортной системы ЗОКИИ

Как протокольные блоки данных выступают вершины гиперграфа. В модели они подробно описываются.

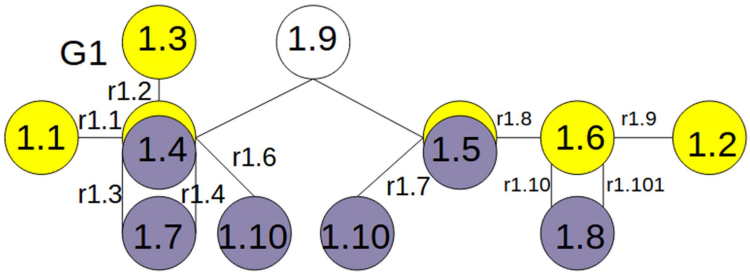

Рис. 6 Граф для моделирования VLAN, ARP объекта критической информационной инфраструктуры

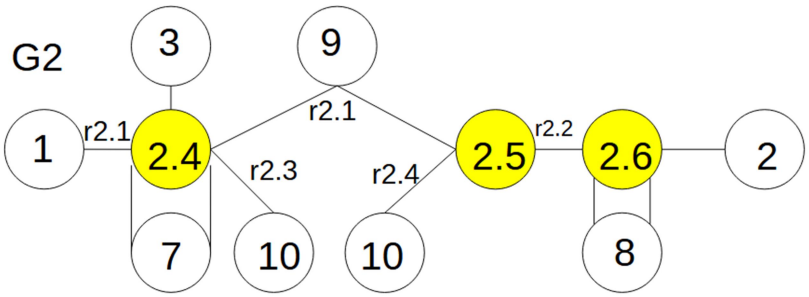

Рис. 7 Граф G2 – топология работы протокола RSTP объекта критической инфраструктуры

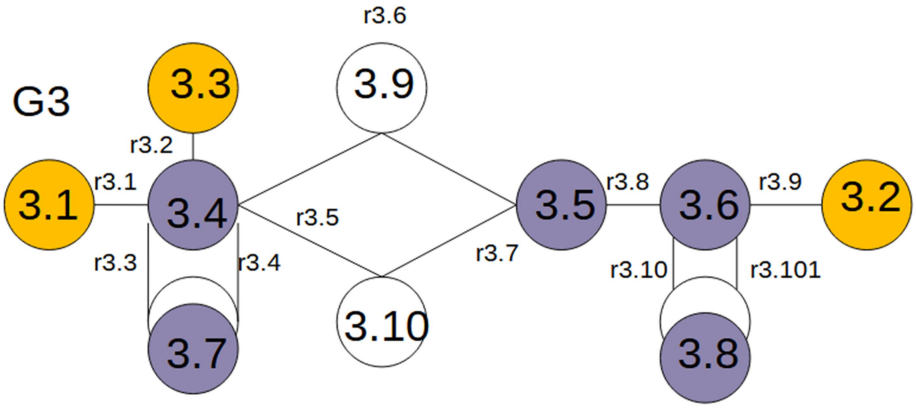

Рис. 8 Граф G3 – топология работы протоколов уровня ICMP, IP критических объектов инфраструктуры

В планируемой модели вершины графов – блоки данных протокольного типа (БДП), работающие на разных уровнях OSI. Взаимодействие (способы, методы) подробно описываются на рисунках 9 и 10 [9].

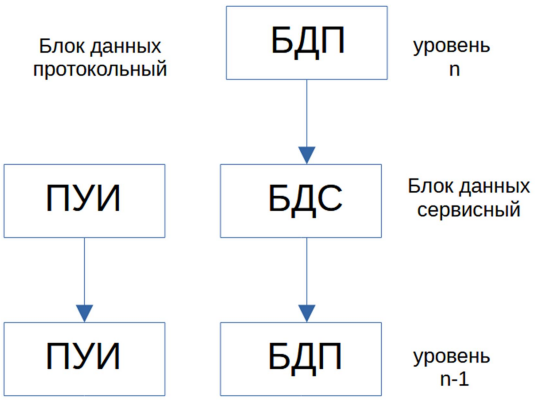

Рис. 9 Схема взаимодействия БДП – в соответствии со стандартами OSI, МЭК 104

На рисунке 10 представлена наглядная схема режимов работы соединение по различным протоколам данных с использованием разных уровней OSI. Представленная иллюстрация предполагает следующие типы соединений:

— с установлением соединения (подключение, транспорт трафика, закрытие соединения/SYN, SYN-ACK, ACK);
— без установления соединения;
— ретрансляция данных;
— дуплексная/полудуплексная передача.

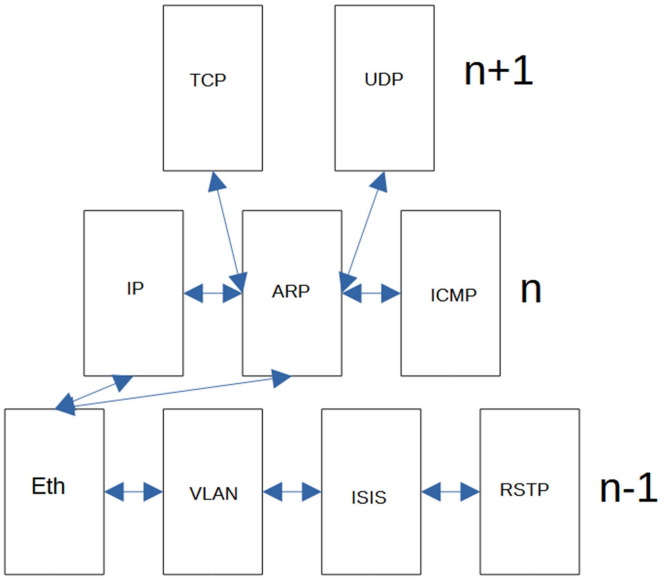

Рис. 10 Схема взаимодействия объектов, работающих на разных уровнях модели OSI

Моделирование иерархии инфраструктуры КСПД с использованием виртуальных машин и iperf

Предприятие планирует закупить и разместить в разных регионах межсетевые экраны usergate d200, c100. Оборудование этого класса, относящееся к категории NGFW, предполагает возможность объединения офисов в режиме Site-to-Site. Это позволит решить задачу передачи телеметрии от станков ЧПУ, относящихся к категории ЗОКИИ, к серверу управления [8].

Для проверки стабильности работы используем виртуальные машины с операционной системой usergate 6.1.8 на базе системы виртуализации esxi 6.7u1. Проверка передачи трафика будет выполняться с помощью утилиты iperf3. Она позволит удостовериться в качестве соединения. Установим утилиту на операционную систему Linux. Iperf server – выступает в качестве серверной части принимающий запрос. Iperf client – клиент, отправляет запрос [11].

Для тестирования построим VPN-туннель типа Site-to-Site между двумя usergate. Маркировка портов, зон, каналов представлена на рисунке 11. Алгоритм настройки интерфейсов, маршрутов предоставлен вендором.

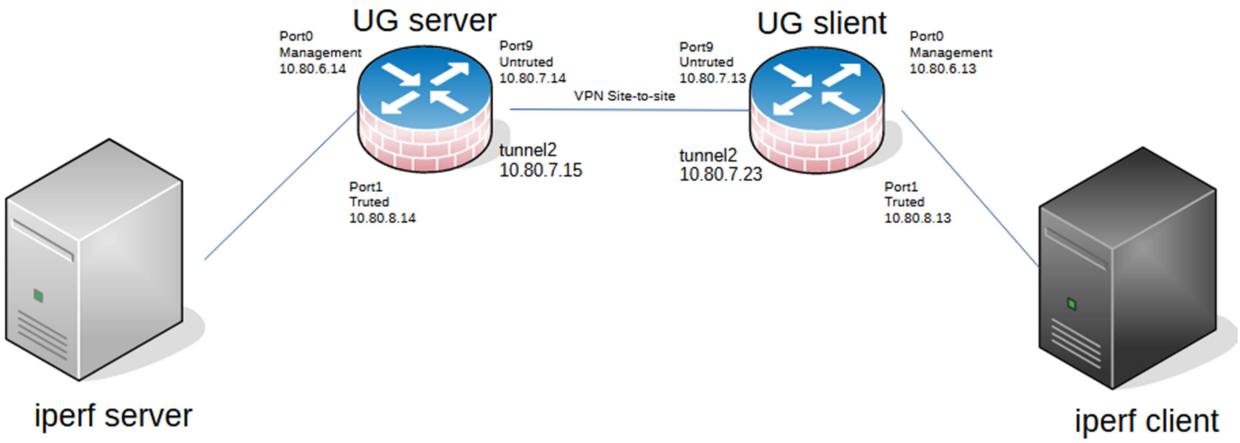

Рис. 11 Схема построения VPN КСПД на базе usergate

Конфигурация интерфейса VPN сервера выполнена через CLI. Вывод конфигурации представлена на рисунке 12. Аналогичные настройки использованы для ввода в эксплуатацию usergate работающего как клиент. Дополнительно прописаны маршруты с шлюзами для транспорта трафика из одной подсети в другую.

```
UTM> iface list port0 port1 port9
Interface "port0" / adapter / enabled: True / active: True / MTU: 1500 / Speed: 10000
Zone: Management (ID=1)
Type: L3
Addresses: 10.80.6.14/24 / mode: static
MAC: 00:0c:29:03:a2:2b

Interface "port1" / adapter / enabled: True / active: True / MTU: 1500 / Speed: 10000
Zone: Trusted (ID=2)
Type: L3
Addresses: 10.80.8.14/24 / mode: static
MAC: 00:0c:29:03:a2:35

Interface "port9" / adapter / enabled: True / active: True / MTU: 1500 / Speed: 10000
Zone: Untrusted (ID=3)
Type: L3
Addresses: 10.80.7.14/24 / mode: static
MAC: 00:0c:29:03:a2:85
```

Рис. 12 Настройки конфигурации сетевых интерфейсов usergate

Два сервера под управлением отечественной операционной системы Astra Linux SE 1.7.3 будут использованы для нагрузочного тестирования. Утилита iperf3 позволит определить скорость передачи данных по созданному каналу связи VPN. В качестве тест-сервера выступит iperf-server – он будет принимать входящее соединение. Запуск приема трафика выполняется командой sudo iperf3 –s (запускается на сервере). Для отправки трафика используется команда sudo iperf3 –c. Запуск выполняется на клиенте. Результат отправки представлена на рисунке 13.

```
root@iperf-client:/home/user/iperf# iperf3 -c 10.80.8.40
Connecting to host 10.80.8.40, port 5201
[  5] local 10.80.8.41 port 54476 connected to 10.80.8.40 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  3.44 GBytes  29.5 Gbits/sec    0   2.00 MBytes
[  5]   1.00-2.00   sec  3.67 GBytes  31.5 Gbits/sec    0   3.11 MBytes
[  5]   2.00-3.00   sec  3.12 GBytes  26.8 Gbits/sec  489   1.86 MBytes
[  5]   3.00-4.00   sec  3.01 GBytes  25.8 Gbits/sec    3   2.38 MBytes
[  5]   4.00-5.00   sec  2.94 GBytes  25.2 Gbits/sec  149   2.05 MBytes
[  5]   5.00-6.00   sec  2.78 GBytes  23.9 Gbits/sec    9   2.14 MBytes
[  5]   6.00-7.00   sec  2.58 GBytes  22.2 Gbits/sec    9   2.22 MBytes
[  5]   7.00-8.00   sec  2.66 GBytes  22.9 Gbits/sec   26   1.67 MBytes
[  5]   8.00-9.00   sec  2.59 GBytes  22.3 Gbits/sec   12   2.03 MBytes
[  5]   9.00-10.00  sec  2.71 GBytes  23.3 Gbits/sec    2   2.17 MBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  29.5 GBytes  25.3 Gbits/sec  699             sender
[  5]   0.00-10.00  sec  29.5 GBytes  25.3 Gbits/sec                  receiver

iperf Done.
root@iperf-client:/home/user/iperf#
```

Рис. 13 Результат отправки трафика с клиента

Результат отправки трафика можно увидеть в терминале сервера на рисунке №14.

```
root@iperf-server:/home/user# iperf3 -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 10.80.8.41, port 54464
[  5] local 10.80.8.40 port 5201 connected to 10.80.8.41 port 54476
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec  3.43 GBytes  29.5 Gbits/sec
[  5]   1.00-2.00   sec  3.68 GBytes  31.6 Gbits/sec
[  5]   2.00-3.00   sec  3.12 GBytes  26.8 Gbits/sec
[  5]   3.00-4.00   sec  3.01 GBytes  25.8 Gbits/sec
[  5]   4.00-5.00   sec  2.94 GBytes  25.2 Gbits/sec
[  5]   5.00-6.00   sec  2.78 GBytes  23.9 Gbits/sec
[  5]   6.00-7.00   sec  2.58 GBytes  22.2 Gbits/sec
[  5]   7.00-8.00   sec  2.66 GBytes  22.9 Gbits/sec
[  5]   8.00-9.00   sec  2.59 GBytes  22.3 Gbits/sec
[  5]   9.00-10.00  sec  2.71 GBytes  23.3 Gbits/sec
[  5]  10.00-10.00  sec  1.37 MBytes  11.5 Gbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.00  sec  29.5 GBytes  25.3 Gbits/sec                  receiver
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

Рис. 14 Результат отправки трафика

Вывод из терминала на рисунке 12 и 13 говорит о практически полном отсутствии падения скорости передачи между сервером и клиентом при прохождении трафика через промежуточные межсетевые экраны с использованием VPN [12]. Что подтверждает заявление разработчика об отсутствии снижения скорости при построении сети передачи данных VPN. Аналогичные результаты были достигнуты при работе на реальном оборудовании: был поднят VPN канал между устройствами usergate d200, выполнены аналогичные испытания с использованием опорной сети провайдера [13].

Заключение

Использование для построения модели ЗОКИИ информационных, автоматизированных систем управления иерархической модели сетей Петри, гиперсетей позволило подтвердить предположения о влиянии протокольных блоков данных на устойчивость к компьютерным атакам. Создав математические модели объектов критической инфраструктуры возможно рассчитать вероятность успешности компьютерной атаки, получить информацию о динамике её развития при изменении параметров самого КИИ [14].

Используя математические объекты и стенды становится возможно оценить производительность оборудования, получить количественные показатели оценки защищенности под воздействием КА.

Литература

1. Гурина Л. А. Оценка киберустойчивости системы оперативно-диспетчерского управления ЭЭС // Вопросы кибербезопасности, 2022. № 3(48), С.18–26. DOI: 10.21681/2311-3456-2022-3-23-31.
2. Осипенко А. А., Чирушкин К. А., Скоробогатов С. Ю., Жданова И. М., Корчевной П. П. Моделирование компьютерных атак на программно-конфигурируемые сети на основе преобразования стохастических сетей //Известия Тульского государственного университета. Технические науки. 2023. № 2. С. 274–281.
3. Зегжда Д. П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. – Москва: Горячая линия – Телеком. 2023. – 500с. – ISBN 978-5-9912-0827-7.
4. Колосок И. Н., Гурина Л. А. Оценка показателей киберустойчивости систем сбора и обработки информации в ЭЭС на основе полумарковских моделей // Вопросы кибербезопасности, 2021, № 6(46), С. 2-11. DOI: 10.21681/2311-3456-2021-6-2-11.
5. Amassing the Security: An Enhanced Authentication Protocol for Drone Communications over 5G Networks / Tsuyang Wu, Xinglan Guo,Yehcheng Chen, Saru Kumari and Chienming Chen // Drones 2022– 6.– 10.
6. Борисов К.В., Любушкина И.Е., Панасенко С.П. и др. Способ, система и устройство криптографической защиты каналов связи беспилотных авиационных комплексов // Патент №2704268, опубликован 25.10.2019 — https://i.moscow/patents/ru2704268c1_20191025.
7. Павленко Е.Ю. Распознавание киберугроз на адаптивную сетевую топологию крупномасштабных систем на основе рекуррентной нейронной сети / Е.Ю. Павленко, Н.В. Гололобов, Д.С. Лаврова, А.В. Козачок // Вопросы кибербезопасности. – 2022. -№6(52). – С. 93-99.
8. Шелухин О. И. Модификация алгоритма обнаружения сетевых атак методом фиксации скачков фрактальной размерности в режиме Online / О. И. Шелухин, С. Ю. Рыбаков, А. В. Ванюшина // Труды учебных заведений связи. – 2022. – Т. 8. – №. 3. – С. 117-126.
9. Tangade S., Kumaar R. A., Malavika S., Monisha S., & Azam F. Detection of Malicious Nodes in Flying Ad-hoc Network with Supervised Machine Learning. In 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE).– 2022. – Pp. 1-5. IEEE.
10. Кононов Р. В. Многоклассовая классификация сетевых атак методами интеллектуального анализа / Р. В. Кононов, О. И. Шелухин // Телекоммуникации и информационные технологии. – 2022. – Т. 9, № 1. – С. 11-16. – EDN AMBLME.
11. Гайдук К.А., Исхаков А.Ю. К вопросу о реализации алгоритмов выявления внутренних угроз с применением машинного обучения // Вестник СибГУТИ. – 2022. – № 16(4). – С. 80-95. – DOI: 10.55648/1998-6920-2022-16-4-80-95.
12. Язов Ю. К. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Санкт-Петербург: Наукоемкие технологии, 2023. – 258 с.
13. Бутрик Е.Е. Подход к определению актуальных угроз безопасности информации в автоматизированных системах управления технологическими процессами с применением банка данных

угроз безопасности информации ФСТЭК России / Е.Е.Бутрик, С.В.Соловьев // Информация и безопасность. – Воронеж,2018. – Выпуск 19 (2). – с.203 – 210.

14. Соловьев С. В. Информационное обеспечение деятельности по технической защите информации / С.В. Соловьев, Ю.К. Язов / Вопросы кибербезопасности. 2021, №1 (41), с. 69–79. DOI: 10.21681/2311-3456-2021-1-69-79.

15. Коцыняк, М.А. Математическая модель таргетированной компьютерной атаки / М.А. Коцыняк, О.С. Лаута, Д.А. Иванов // Наукоемкие технологии в космических исследованиях Земли. – 2019. – Т. 11, № 2. – С. 73-81. – DOI 10.24411/2409-5419-2018-10261.

16. Бугайский, К.А. Расширенная модель открытых систем (Часть 3) / К.А. Бугайский, Б.О. Дерябин, К.В. Табаков, Е.С. Храмченкова, С.О. Цепенда // Информация и безопасность. – 2022. – Т. 25, № 4. – С. 501-512.

17. Лившиц И. И., Бакшеев А.С. Исследование методик контроля уровня защищенности информации на объектах критической информационной инфраструктуры / И. И. Лившиц, А. С. Бакшеев. // Вопросы кибербезопасности. — 2022. — № 6(52). — С. 40-52.

18. Робертович А.В., Табакаева В.А., Селифанов В. В. Разработка методики аудита кибербезопасности государственных информационных систем, относящихся к значимым объектам критической информационной инфраструктуры, функционирующих на базе центров обработки данных // Интерэкспо Гео-Сибирь. 2020. №1.

19. Макаренко С.И., Смирнов Г.Е. Анализ стандартов и методик тестирования на проникновение // Системы управления, связи и безопасности. 2020. №4.

20. Нестеровский О.И., Пашковская Е.С., Бутрик Е.Е. Методический подход к организации проведения контроля защищенности информации на объектах критической информационной инфраструктуры // Вестник ВИ МВД России. — 2021. — № 2. — С.126-133.

Development of a methodology for analyzing the resilience of ZOKIA objects to computer attacks by modeling using the concept of Petri nets

DMITRY A. LYUBIMENKO
Deputy Director General for Information Security of Akvamash Software LLC, Volgograd, Russia, d.lyubimenko@aquamash.ru

ABSTRACT

Introduction: Development of a methodology for analyzing the stability of significant objects of critical information infrastructure to hacking, computer attacks, and the effects of malicious computer programs. The purpose of the study is to perform modeling of objects of significant critical information infrastructure using the concept of building Petri nets, hypernetworks. **The purpose of the study:** Using the concept of building Petri nets, hypernetworks perform modeling of objects of significant critical information infrastructure. **Results:** The proposed methodology for constructing a model of ZOKIA objects will make it possible to accurately determine the probability of a computer attack, and develop a scheme of resistance to non-legitimate influence. The developed method of constructing the model takes into account the specifics of the objects of the research: the features of communication, the construction of a corporate data transmission network (KSPD), the dynamics of operation. All of these factors affect the system's resistance to hacking. The task of assessing the protection and ensuring the information security of the ZOKIA is being solved. The methodology reduces dependence on subjective expert assessments, closes the issue of compliance with legal requirements in terms of meeting the requirements of the Federal Service for Technical and Export Control. The annual tightening of the rules for the operation of critical infrastructure facilities requires a special approach. The operation of the technique is an organizational measure of protection against intruders. **Practical significance:** the ability to model parametric models of critical information infrastructure objects with high accuracy. When modeling, estimates of the security of communication and infrastructure parameters of the object itself are taken into account. The independence of assessing the state of information security of corporate data transmission networks, other types of facilities (automated control systems, automated process control systems) of subjects working in the defense industry is significantly increased. This is especially important before scheduled and unscheduled inspections by regulators (FSTEC, FSB). Following the methodology reduces the likelihood of fines being imposed on the head of the enterprise, an information security specialist.

Keywords: information security, ZOKII, CII, mathematical modeling, stability

REFERENCES

1. Gurina L. A. Assessment of cyber stability of the EES operational dispatch control system // Issues of cybersecurity, 2022. No. 3(48), pp.18-26. DOI: 10.21681/2311-3456-2022-3-23-31.

2. Osipenko A. A., Chirushkin K. A., Skorobogatov S. Yu., Zhdanova I. M., Korchevnoy P. P. Modeling of computer systems attacks on software-configurable networks based on the transformation of stochastic networks //Proceedings of Tula State University. Technical sciences. 2023. No. 2. pp. 274-281.

3. Zegzhda D. P. Cybersecurity of the digital industry. Theory and practice of functional resistance to cyber attacks / Edited by Professor of the Russian Academy of Sciences, Doctor of Technical Sciences D.P. Zegreda. – Moscow: Hotline – Telecom. 2023. – 500s. – ISBN 978-5-9912-0827-7.

4. Kolosok I. N., Gurina L. A. Assessment of cyber stability indicators of information collection and processing systems in the EES based on semi-Markov models // Cybersecurity Issues, 2021, No. 6(46), pp. 2-11. DOI: 10.21681/2311-3456-2021-6-2-11.

5. Amassing the Security: An Enhanced Authentication Protocol for Drone Communications over 5G Networks / Tsuyang Wu, Xinglan Guo,Yehcheng Chen, Saru Kumari and Chienming Chen // Drones 2022– 6.– 10.

6. Borisov K.V., Lyubushkina I.E., Panasenko S.P., etc. Method, system and device for cryptographic protection of communication channels of unmanned aircraft complexes // Patent No.2704268, published 10/25/2019 — https://i.moscow/patents/ru2704268c1_20191025 .

7. Pavlenko E.Y. Recognition of cyber threats on the adaptive network topology of large-scale systems based on a recurrent neural network / E.Y. Pavlenko, N.V. Gololobov, D.S. Lavrova, A.V. Kozachok // Issues of cybersecurity. – 2022. -№6(52). – Pp. 93-99.

8. Shelukhin O. I. Modification of the algorithm for detecting network attacks by fixing jumps of fractal dimension in Online mode / O. I. Shelukhin, C. Yu. Rybakov, A.V. Vanyushina // Proceedings of educational institutions of communications. – 2022. – Vol. 8. – No. 3. – pp. 117-126.

9. Tangade S., Kumaar R. A., Malavika S., Monisha S., & Azam F. Detection of Malicious Nodes in Flying Ad-hoc Network with Supervised Machine Learning. In 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE).– 2022. – Pp. 1-5. IEEE.

10. Kononov R. V. Multiclass classification of network attacks by methods of intellectual analysis / R. V. Kononov, O. I. Shelukhin // Telecommunications and information technology. - 2022. – Vol. 9, No. 1. – pp. 11-16. – EDN AMBLME.

11. Gaiduk K.A., Iskhakov A.Yu. On the implementation of algorithms for detecting internal threats using machine learning // Bulletin of SibGUTI. – 2022. – № 16(4). – Pp. 80-95. – DOI: 10.55648/1998-6920-2022-16-4-80-95.

12. Yazov Yu. K. Methodology for evaluating the effectiveness of information protection in information systems from unauthorized access: monograph / Yu.K. Yazov, S.V. Solovyov. – St. Petersburg: High-tech technologies, 2023. – 258 p.

13. Butrik E.E. Approach to the definition of actual threats to information security in automated process control systems using the database of threats to information security of the Federal State Technical Committee of Russia / E.E.Butrik, S.V.Solovyov // Information and Security. – Voronezh, 2018. – Issue 19 (2). – pp.203-210.

14. Solovyov S. V. Information support for the technical protection of information / S.V. Solovyov, Yu.K. Yazov / Cybersecurity issues. 2021, No.1 (41), pp. 69-79. DOI: 10.21681/2311-3456-2021-1-69-79.

15. Kotsynyak, M.A. Mathematical model of targeted computer attack / M.A. Kotsynyak, O.S. Lauta, D.A. Ivanov // High–tech technologies in space research of the Earth. – 2019. – Vol. 11, No. 2. – pp. 73-81. - DOI 10.24411/2409-5419-2018-10261.

16. Bugaisky, K.A. Extended model open systems (Part 3) / K.A. Bugaisky, B.O. Deryabin, K.V. Tabakov, E.S. Khramchenkova, S.O. Tsependa // Information and security. - 2022. – Vol. 25, No. 4. – pp. 501-512.

17. Livshits I. I., Baksheev A.S. Investigation of methods for monitoring the level of information security at critical information infrastructure facilities / I. I. Livshits, A. S. Baksheev. // Cybersecurity issues. — 2022. — № 6(52). — Pp. 40-52.

18. Robertovich A.V., Tabakaeva V.A., Selifanov V. V. Development of a methodology for auditing cybersecurity of state information systems related to significant objects of critical information infrastructure operating on the basis of data processing centers // Interexpo Geo-Siberia. 2020. №1.

19. Makarenko S.I., Smirnov G.E. Analysis of standards and methods of penetration testing // Control systems, communications and security. 2020. No.4.

20. Nesterovsky O.I., Pashkovskaya E.S., Butrik E.E. Methodological approach to the organization of information security control at critical information infrastructure facilities // Bulletin of the Ministry of Internal Affairs of Russia. — 2021. — No. 2. — pp.126-133.