УДК 004.056.5

# МЕТОДОЛОГИЯ МОДЕЛИРОВАНИЯ И ОЦЕНКИ ЗАЩИЩЕННОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

**Д.А. Васинев (Орел)**

## Введение

Актуальность вопросов обеспечения информационной безопасности для информационных систем (ИС), информационно-телекоммуникационных сетей (ИТС), автоматизированных систем управления (АСУТП) критических информационных инфраструктур (КИИ), функционирующих в критически важных отраслях деятельности государства в медицине, образовании, промышленности, энергетике поясняется отраслевой принадлежностью объектов атак, что говорит о продолжающемся информационном противоборстве. Среди прочих, целью нарушителя является объекты КИИ, причем уровень деструктивной действий нарушителя на коммуникационную инфраструктуру говорит о сетевых угрозах, при этом преимущественно высоких и критических уровнях, воздействия нарушителя, проявляющихся в атаках на КИИ, что представлено в отчетах о известных инцидентах [1-3].

В качестве составных элементов КИИ выступают распределенные фрагменты сетей, центры обработки данных (ЦОД), автоматизированные системы управления, объединенные в единую распределенную ИТС организации, пример обобщённого представления распределенной КИИ представлен на рисунке 1. Существующие особенности построения коммуникационной инфраструктуры технологически достаточно разнообразны, однако общими требованиями является применение технологий резервирования, отказоустойчивости, виртуальных частных сетей (VPN), обеспечение устойчивости в условиях воздействия КА. Кроме того, современные условия функционирования технических систем предполагают применение отечественного коммуникационного оборудования, средств защиты для проектирования новых и импортозамещения существующих фрагментов КИИ, в этих условиях исследования ИБ в области оценки защищенности и устойчивости КИИ в условиях воздействия на нее КА является актуальной задачей.

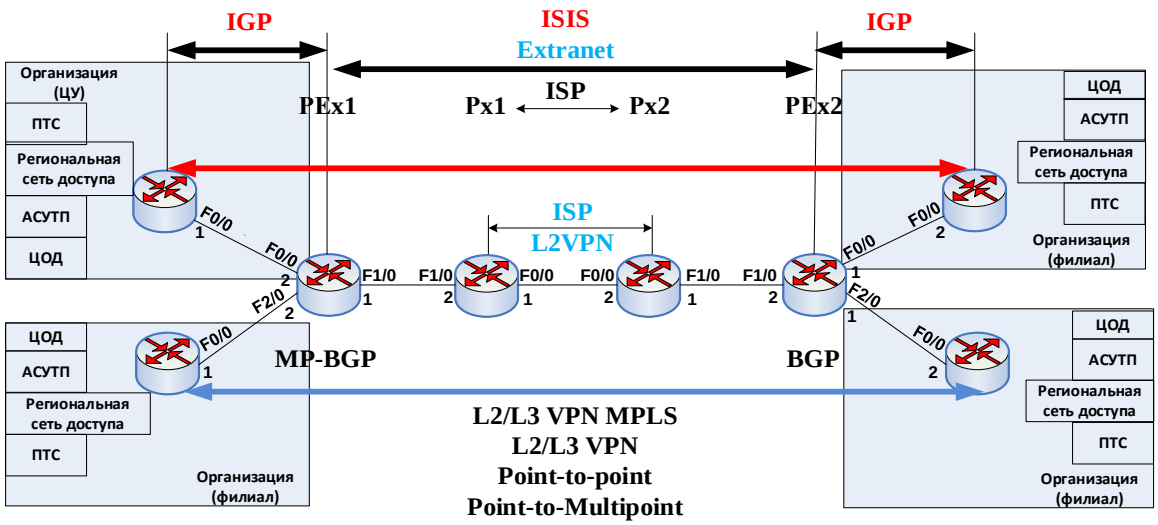


Рис. 1. Формирование распределенной инфраструктуры для объектов ИС, АСУТП, ИТС КИИ

Воздействие нарушителя на распределенную ИТС обусловлено инфраструктурными, коммуникационными особенностями организации каналов связи, предлагаемых оператором связи, на основе которого осуществляется организация взаимодействия между распределенными филиалами телекоммуникационных объектов КИИ (представлено на рисунке 2). Сетевые, транспортные и управляющими протоколы, которые применяются в коммуникационных инфраструктурах для передачи данных (такие как Ethernet, ICMP, IP, TCP, SNMP, Modbus, MMS и Goose), для которых помимо иерархических – коммуникационных особенностей можно выделить конфигурационные компоненты формирования инфраструктур, также могут быть причиной снижения защищенности объекта – в связи с воздействием нарушителя, или неквалифицированных действий персонала в распределенных фрагментах ИТС.

В настоящее время при обеспечении информационной безопасности (ИБ) объектов КИИ наряду со свойствами целостности, доступности, конфиденциальности, формируется понятие устойчивости КИ как в нормативных документах [4], так и в известных исследованиях в области ИБ, ряд авторов рассматривает свойство устойчивости объектов коммуникационной инфраструктуры от компьютерных атак [5-8] как свойство защищенности объекта.

Решение задачи устойчивости функционирования КИИ авторы [5-8] связывают с возможностями ее противостоять компьютерным атакам в основном методами резервирования на структурном – физическом уровне. В рамках исследования делается предположение о возможностях получения оценок устойчивости объектов КИИ при противодействии КА в логических каналах методом динамического изменения характеристика, что соответствует функциональному варианту обеспечения устойчивости. Примером логического резервирования могут быть параметры самого логического канала, типы применяемых виртуальных частных сетей (VPN), топология соединения, маршрутная информация, скорость передачи, качество обслуживания. Все это связано с технологическими особенностями построения, применимыми технологиями, иерархическими особенностями построения КИИ, вариант которой представлен на рисунке 2.

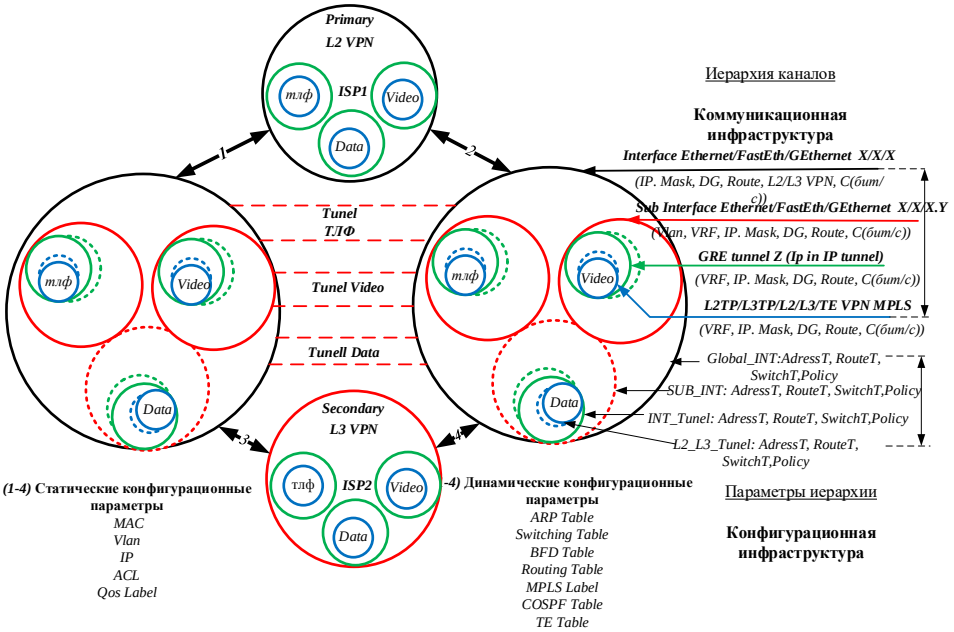


Рис.2. Вариант иерархической, вложенной коммуникационной инфраструктуры для моделирования распределенной инфраструктуры ИС, АСУТП, ИТС, объектов КИИ

Технологические особенности связаны с применением различных вариантов туннелирования (L2, L3 VPN), при формировании распределенной ИТС, а также с применением как физически зарезервированных каналов, так и логического резервирования на основе следующих технологий и протоколов: Rapid spanning tree protocol (RSTP), Virtual router redundancy protocol (VRRP), Biderectional forwarding detection (BFD), Routing, MPLS Fast reroute FastRR.

Очевидно, что логическая структура каналов связи для КИИ имеет иерархическую особенность формирования и построения, обусловленную применением коммуникационных и конфигурационных параметров в КИИ рассматриваемых объектов (ИС, АСУТП, ИТС), функционирующих в единой распределенной сети организации.

Для нарушителя продолжат представлять интерес сетевые воздействия преимущественно с высоким и критическим уровнем опасности (рисунок 3).

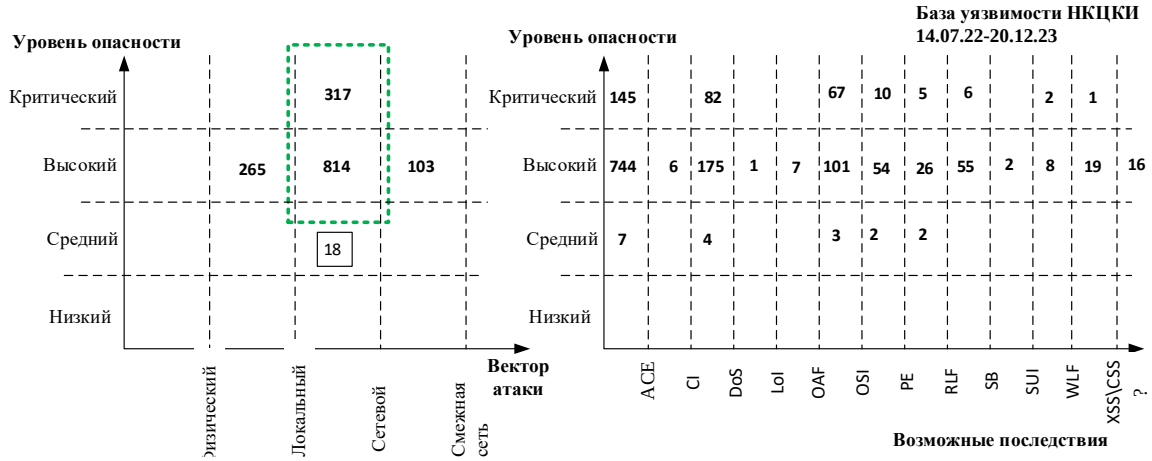


Рис. 3 – Уровень опасности и сетевая направленность уязвимостей

В условиях воздействия на коммуникационную инфраструктуру объекта КИИ сетевых воздействия нарушителя способы оценки защищенности основаны на знании сигнатуры угрозы и сводятся к правилу оценки защищенности только известных угроз, как представлено на рисунке 4. В таких условиях нарушитель, работающий в известном пространстве состояний объекта КИИ, обладает $2^m$ параметрами для воздействия на объект КИИ. Такие возможности нарушителя позволяют изменять сигнатуры, формировать новые, ранее неизвестные воздействия. Таким образом, подход по обеспечению защищенности объекта КИИ на основе сигнатурных методов всегда отстает по времени от воздействия нарушителя, что создает предпосылки нахождения объекта КИИ в незащищенном состоянии.

Формирование сигнатур на основе существующих БД сигнатур методами машинного обучения является перспективным направлением, требовательным к исходным данным о состоянии объекта КИИ в защищенном, незащищенном состоянии. Причем, применение для этого знаний о параметрах функционировании самого объекта КИИ является ключевым фактором, требующим учета в разрабатываемых моделях.

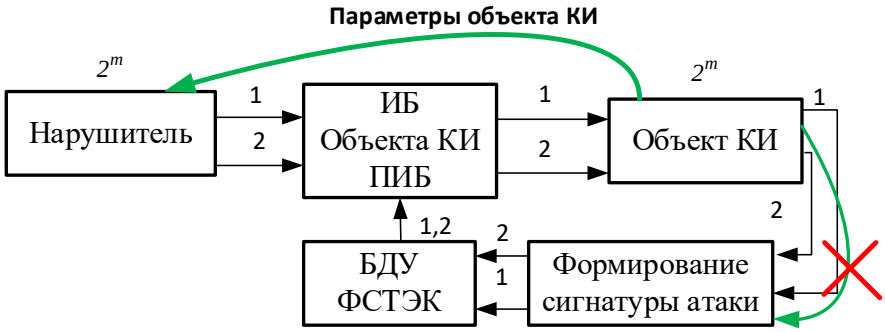


Рис. 4 – Существующая модель формирования политики безопасности на объектах КИИ

Решением сложившегося противоречия между многообразием воздействия нарушителя и существующими возможностями методов и средств обеспечения информационной безопасности является учет параметров объекта КИИ в формировании политики информационной безопасности объекта (представлено на рисунке 5).

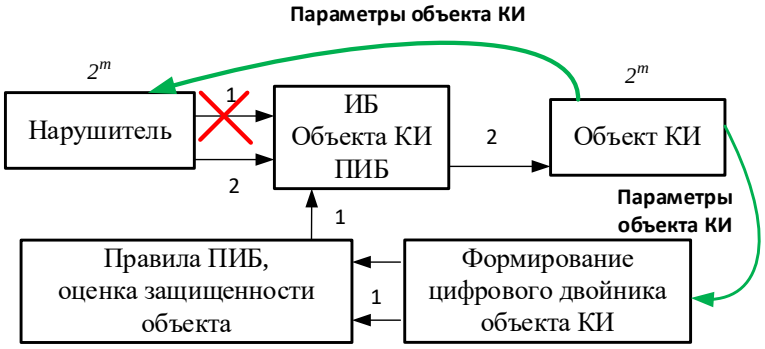


Рис. 5 – Предлагаемый вариант формирования политики безопасности оценки защищенности на объектах КИИ

В основу предлагаемого метода оценки защищенности и формирования политики ИБ объекта КИИ закладывается построение на основе данных о параметрах функционирования объекта КИИ параметрически точного цифрового двойника. В основе цифрового двойника лежит комплекс имитационных моделей на основе вложенных раскрашенных сетей Петри, а также полунатурных моделей. Комплекс моделей цифрового двойника включает в себя модель объекта КИИ, модели каналов связи, комплекс взаимоувязанных моделей, связанных с формированием политики ИБ, анализом защищенности и действиями нарушителя (см. рисунки 8, 11-14).

**Теоретические основы оценки защищенности коммуникационной инфраструктуры объектов КИИ**

Формирование множества известных и неизвестных угроз (см. рисунок 6) относительно возможностей средств обеспечения информационной безопасности основано на правилах формирования множества «разрешено», множества «запрещено», множества «все остальное» для средств формирования политики информационной безопасности.

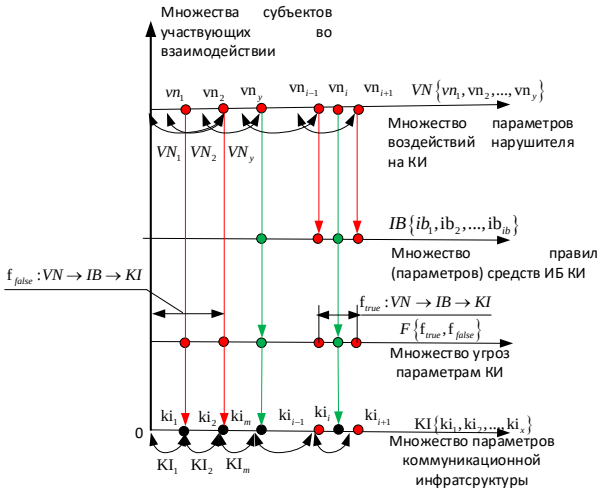


Рис. 6 – Пример формирования множеств известных угроз, а также множеств неизвестных угроз для объектов КИИ

В основе предлагаемого в рамках работы метода оценки защищенности лежит гипотеза о разделении множества угроз на два непересекающихся класса относительно возможностей средств обеспечения информационной безопасности: $f_{true}$ – множество устранимых существующими средствами ИБ угроз, $f_{false}$ – множество неустранимых, в том числе, неизвестных угроз ИБ (как представлено на рисунке 7).

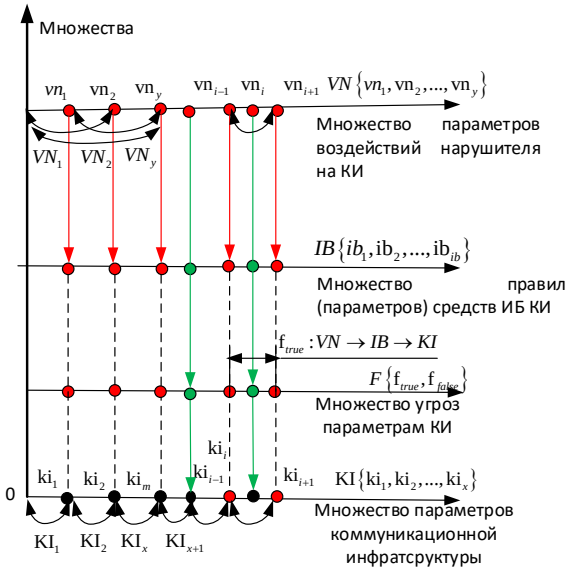


Рис. 7 – Пример обеспечения устойчивости коммуникационной инфраструктуры

Определение 1 (гипотеза) о безопасности коммуникационной инфраструктуры.

Коммуникационная инфраструктура УК находится в безопасном (защищенном) состоянии $KI$, при воздействии нарушителя множеством параметров $VN$ существует импликация $VN_1 \to VN_2 \to VN_y$, таких что $VN_1 \cap VN_2 \cap VN_y \neq 0$, для любого множества параметров воздействия нарушителя $VN$ находятся такие множества параметров $IB$, что существует отображение

$$F : VN \to IB \to KI,$$

$$(\mathrm{f}_{true}: VN \to IB \to KI, \forall VN, IB, KI \; \exists VN \cap IB = IB \cap KI, VN \cap KI \neq 0;$$
$$\mathrm{f}_{false}: VN \to IB \to KI, \forall VN, IB, KI \; \exists VN \cap IB \neq IB \cap KI, VN \cap KI \neq 0)\,.$$

Для сделанных предположений о структуре множества угроз $F\{\mathrm{f}_{true}, \mathrm{f}_{false}\}$, воздействий нарушителя $VN\{vn_1, \mathrm{vn}_2, ..., \mathrm{vn}_y\}$, множества правил политики информационной безопасности, связанных с параметрами средств обеспечения информационной безопасности $IB\{ib_1, \mathrm{ib}_2, ..., \mathrm{ib}_{ib}\}$, множество угроз для коммуникационной инфраструктуры $F\{\mathrm{f}_{true}, \mathrm{f}_{false}\}$, связаны с множеством параметров коммуникационной инфраструктуры $\mathrm{KI}\{\mathrm{ki}_1, \mathrm{ki}_2, ..., \mathrm{ki}_x\}$ непосредственно значениями параметров, правилами настройки этих параметров в средствах ИБ.

Для множества выделенных угроз для коммуникационной инфраструктуры воздействия нарушителя представляют собой пересекающиеся воздействий на параметры коммуникационной инфраструктуры $VN_1, VN_2, VN_3$ (рисунок 7).

Каждое из воздействий нарушителя обрабатывается правилами политики ИБ $IB\{ib_1, \mathrm{ib}_2, ..., \mathrm{ib}_{ib}\}$, причем на каждое воздействие есть свое правило политики ИБ, все воздействия нарушителя парируются средствами ИБ. В таких условиях, с точки зрения политики информационной безопасности, узел защищен, а с точки зрения политик качества обслуживания парируемые угрозы вызывают переполнение полосы пропускания виртуальных каналов, заполнение обслуживающих очередей, деградацию параметров качества обслуживания, в дальнейшем ошибки и отказы направления связи.

В таких условиях для противодействия пересекающемуся множеству воздействия нарушителя, помимо конфигурации средств обеспечения информационной безопасности $VN_1, VN_2, VN_3$, выступает непересекающееся множество параметров конфигураций коммуникационной инфраструктуры $\mathrm{KI}_1, \mathrm{KI}_2, \mathrm{KI}_3$.

В условиях непересекающихся воздействий нарушителя на объект КИИ изменение конфигурации коммуникационной инфраструктуры является параметрическим способом ухода от воздействия нарушителя в условиях функционирования средств информационной безопасности. Если число таких множеств параметров соизмеримо с количеством воздействий нарушителя, объект КИИ будет находиться в защищенном состоянии.

**Метод сквозного моделирования объектов КИИ на основе средств полунатурного и имитационного моделирования**

На основе сформулированных предположений разработаны метод моделирования иерархически сложных телекоммуникационных объектов и метод оценки защищенности на основе учета параметров объекта КИИ.

В работе установлено, что для моделирования вложенных иерархических многопараметрических конструкции с достаточной степенью адекватности применяются раскрашенные вложенные сети Петри. При этом имитационное моделирование позволяет разработать универсальный метод построения имитационных протокольных блоков данных (для различных типов протоколов), учесть коммуникационные и конфигурационные особенности их функционирования,

являющиеся основой метода сквозного моделирования сетей, узлов и комплексов специальной связи (рисунки 8а-8г).

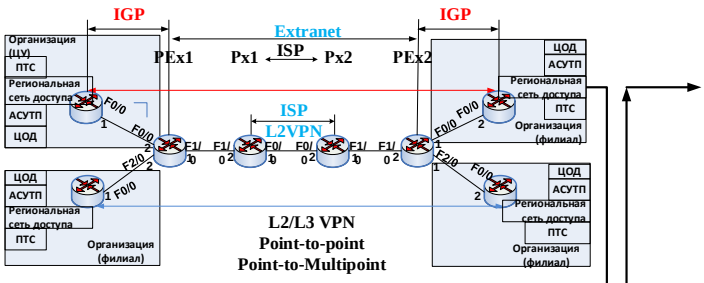


Рис. 8а. Объект моделирования коммуникационной инфраструктуры объекта КИИ

Рис. 8б. Универсальная масштабируемая модель коммуникационной инфраструктуры объекта КИИ на основе средств полунатурного моделирования

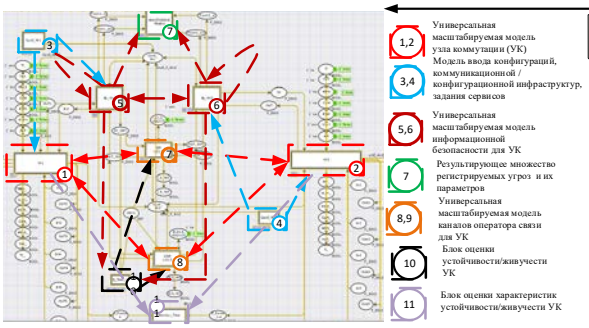


Рис. 8в. Масштабируемая модель на основе сетей Петри для оценки защищенности коммуникационной инфраструктуры объекта КИИ


Рис. 8г. Пример полунатурной масштабируемой модели коммуникационной инфраструктуры объекта КИИ

Рис. 8 – Метод сквозного моделирования объектов КИИ на основе средств полунатурного и имитационного моделирования

Объекты, представленые на рисунке 8, объединены единой логической составляющей – конфигурационными и коммуникационными параметрами. На физическом объекте – конфигурационные и коммуникационные параметры, в полунатурных моделях применяется конфигурация физического объекта с высокой степенью достоверности. Для применения конфигурационных и коммуникационных параметров в средствах имитационного моделирования необходимы дополнительные преобразования, позволяющие из разнообразных типов конфигураций получать параметры для имитационной модели.

Основной задачей, решаемой в методе моделирования коммуникационных инфраструктур, является получение универсальных масштабируемых имитационных и полунатурных модулей, пригодных для моделирования многоуровневых распределенных коммуникационных инфраструктур различных объектов КИИ.

Моделирование многоуровневых коммуникационных инфраструктур связано с особенностями их построения, представленными на рисунке 9.

Основными особенностями, которые легли в основу универсальных масштабируемых модулей для имитационного и полунатурного моделирования, являются внутриуровневое и межуровневое взаимодействие протокольных блоков данных, представленных на рисунке 10.

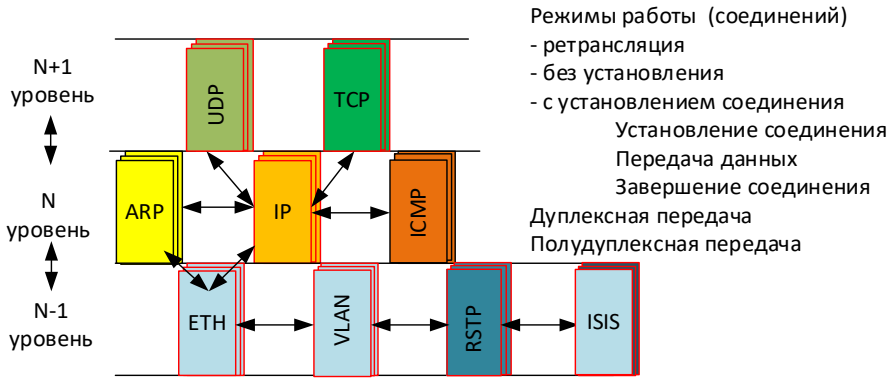


Рис.9 – Вариант взаимодействия объектов различных уровней в соответствии с моделью OSI (7498), X.200, ГОСТ Р ИСО/МЭК 7498-1-99

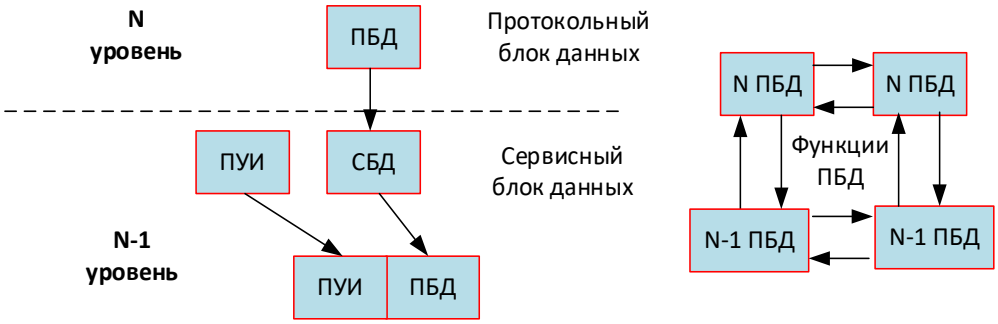


Рис. 10 – Методы, способы взаимодействия ПБД в соответствии с моделью OSI (7498), X.200, ГОСТ Р ИСО/МЭК 7498-1-99

Примеры моделирования вариантов конструкций протокольных блоков данных и особенностей их объединения, представлены на рисунках 11 - 14.

Универсальная масштабируемая модульная конструкция для моделирования коммуникационной системы различного типа (рабочая станция, коммутатор, маршрутизатор) представлена на рисунке 11. Универсальная модульная конструкция, позволяющая моделировать каналы связи оператора связи, представлена на рисунке 12. Универсальная модульная конструкция, позволяющая моделировать работу системы информационной безопасности, системы анализа защищенности, а также действия нарушителя информационной безопасности, представлена на рисунке 13, верхний уровень имитационной модели – на рисунке 14.

На основе предлагаемого метода моделирования объектов КИИ получены точные имитационные модели относительно параметров объектов КИИ. Разработанные модели позволяют осуществлять моделирование политики ИБ, проверку политики ИБ – анализ защищенности, моделирование действий нарушителя. Параметры коммуникационной инфраструктуры являются исходными данными для функционирования модуля ИБ, на основе которого формируются тестовые проверочные конструкции.

Полученные результаты полунатурного и имитационного моделирования позволяют применять их для расчета защищенности объекта КИИ, пример которой представлен в таблицах 1 - 4.

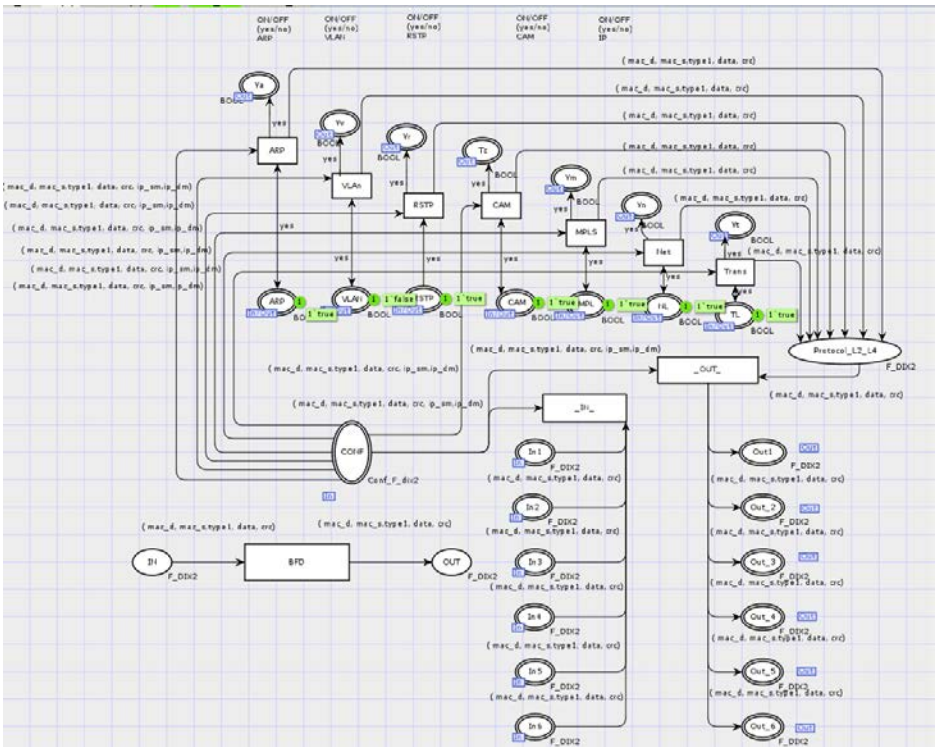

Рис. 11 – Пример универсального масштабируемого модуля для моделирования коммуникационной системы различного типа

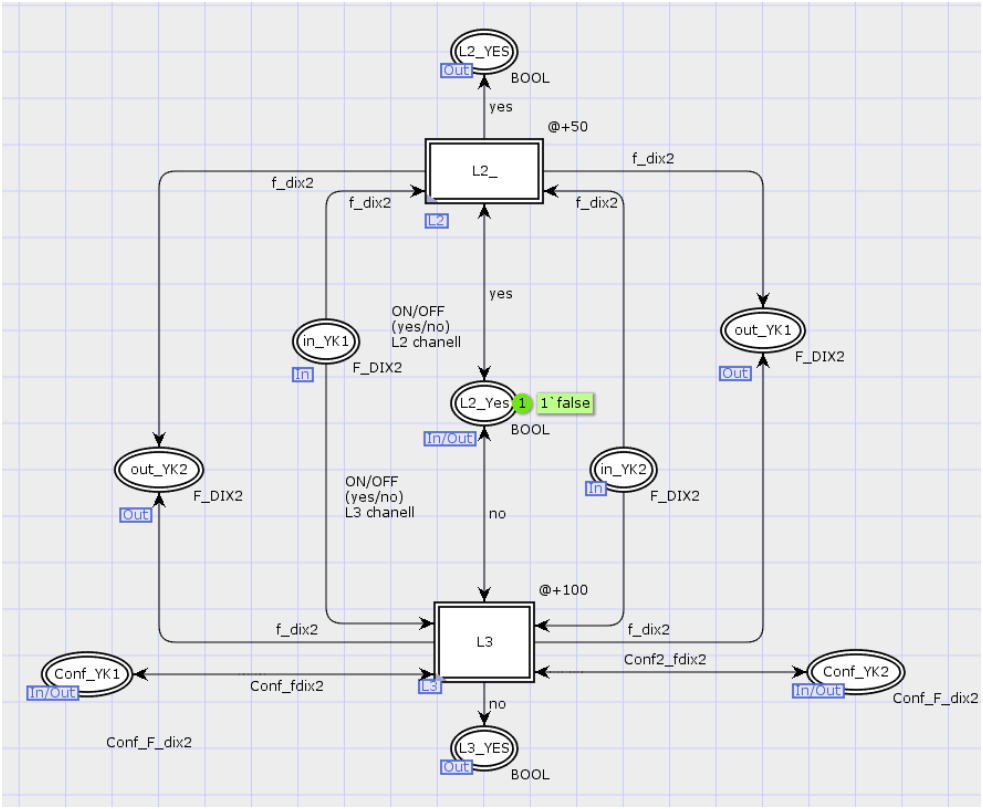


Рис. 12 – Пример универсального модуля для исследования каналов L2/L3 оператора связи

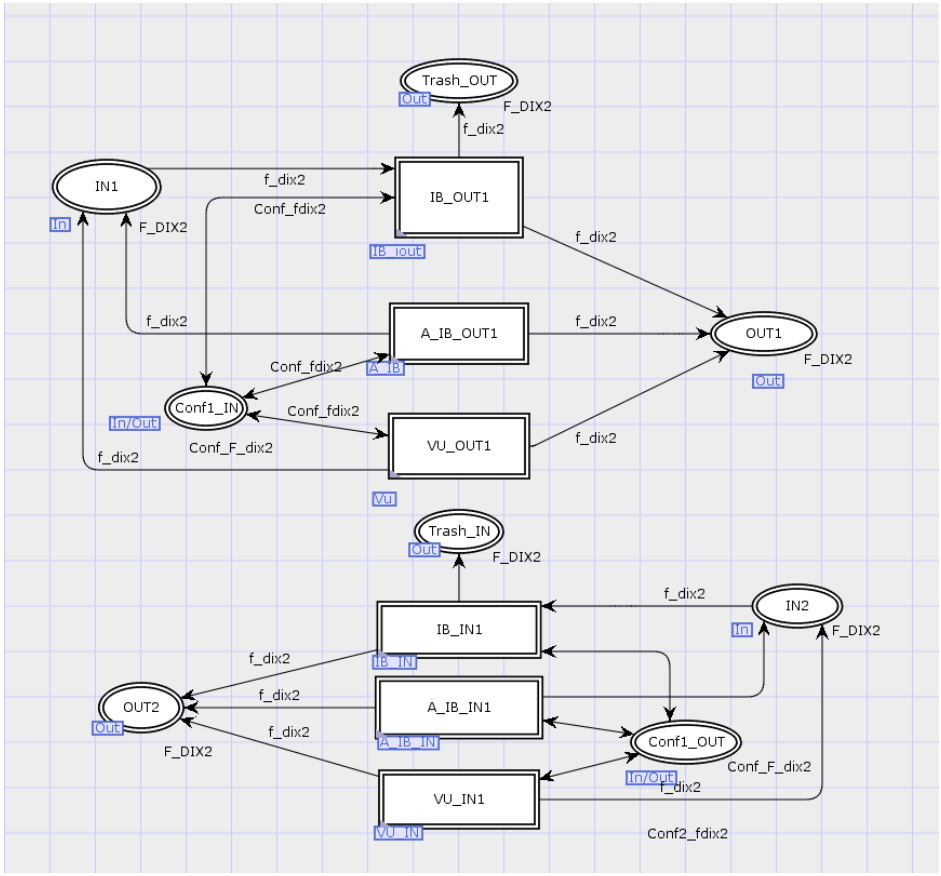


Рис. 13 – Пример модульной конструкции, позволяющей моделировать работу системы информационной безопасности

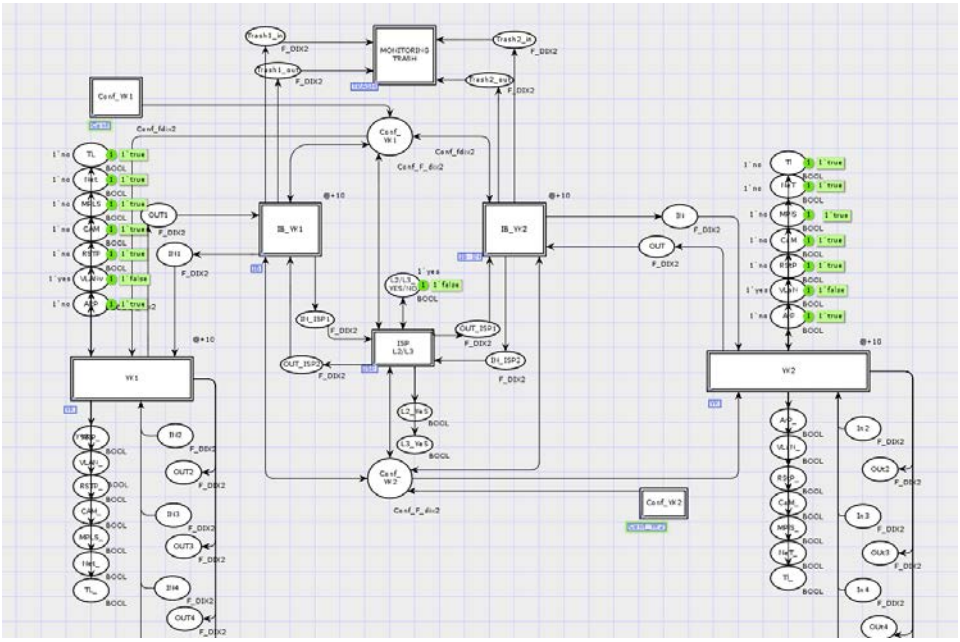

Рис. 14 – Пример иерархической коммуникационной инфраструктуры на примере взаимодействия двух узлов коммутации

Пример расчета основан на оценке защищенности кадра Ethernet DIX2, на размер которого возможно $2^{1518}$ бит воздействий нарушителя. Параметры коммуникационной инфраструктуры позволяют снизить размерность пространства состояний до 5 значений. Снижение пространства состояний стало возможным с учетом параметров: 00:00:00:00:00:02 – macD, 00:00:00:00:00:01 – macS, 11:11:11:1:11:11 – широковещательный; Etype(2): 0x0800 (2048) – Ipv4; 0x8100 (33024) – 802.1q. Пусть правила политики ИБ объекта содержат 2 значения по фильтрации кадров. Проверка работоспособности функционирования политики ИБ относительно параметров объекта КИИ осуществляется не более чем 5 тестовыми запросами, содержащими только проверяемые значения. Анализ защищенности осуществляется на основе $2 \cdot m$ параметров, позволяет проверить работоспособность политики ИБ по верхней и нижней границе. Значения тестовых множеств для рассматриваемого примера представлены в таблице 1.

Таблица 1 – Исходные данные для оценки защищенности объекта КИИ

| Количество параметров (коммуникационных, конфигурационных) | Количество правил политики ИБ объекта | Количество правил для проверки политики ИБ | Количество правил для анализа защищенности одного направления | Количество правил для анализа защищенности с учетом политики ИБ |
|---|---|---|---|---|
| $N_i^{KИ}$ , $N_i^{Cnf}$ | $rule_i^{MsIB}$ | ( $N_i^{KИ} + N_i^{Cnf}$ ) | $2^{(K_{BH_i}^{KИ} + Cnf_{BHi}^{KИ})}$ | $(2 \cdot m + m)$ |
| 5 | 2 | 5 | 10 | 15 |

На основе представленных параметров произведены расчеты на имитационной модели, результаты которых представлены в таблице 2.

Таблица 2 – Результаты функционирования имитационной модели

| Количество пакетов сформированных имитационной моделью | Количество пакетов не соответствующих политике ИБ | Количество пакетов нарушителей КИ, потенциально устранимых средствами политики ИБ $T_{УСТР}^{KИ} \le T_{доп}^{KИ}$ | Количество пакетов нарушителей КИ, неустранимых средствами политики ИБ за время $T_{УСТР}^{N} \ge T_{доп}^{N}$ |
|---|---|---|---|
| $P_i$ | $K_i$ ( $K_i^{KИ}$, $Cnf_i^{KИ}$, $N_i^{KИ}$ ) | $K_{BH_i}^{KИ}$, $Cnf_{BHi}^{KИ}$ | $N_i^{KИ}$ |
| 112 | 50 | 40 | 10 |

При работе имитационной модели было сформировано 112 кадров, из которых число деструктивных кадров – 50, среди которых 40 учитываются политикой ИБ объекта КИИ, а 10 не учитываются по причине отсутствия функциональных возможностей оборудования, необходимостью модернизации самой политики ИБ.

Получение тестовых последовательностей $P_i$ , множество пакетов воздействия нарушителя – угроз коммуникационной инфраструктуре, конфигурациям, неизвестные

относительно возможностей средств информационной безопасности ( $K_i$ ( $K_i^{КИ}$ , $Cnf_i^{КИ}$ , $N_i^{КИ}$ )) – угрозы не прошедших политику ИБ. Выделенное множество угроз $K_i$ содержит угрозы ( $K_{BH_i}^{КИ}$ , $Cnf_{BHi}^{КИ}$ ), устранимые средствами политики ИБ за время $T_{УСТР}^{КИ} \le T_{доп}^{КИ}$ , и угрозы $N_i^{КИ}$ , неизвестные для средств политики ИБ, за время $T_{УСТР}^{N} \ge T_{доп}^{N}$ для коммуникационной инфраструктуры объектов КИИ, как представлено в таблице 2.

Имитационная модель позволяет исследовать поведение объекта КИИ в условиях резервирования физических или логических элементов объекта КИИ. Результаты расчетов коэффициентов резервирования физических и логических элементов объекта КИИ представлены в таблице 3. Верхние границы расчетов значений $F_{доп}$ , $L_{доп}$ обусловлены конечностью ресурса объекта КИИ.

Таблица 3 – Расчет коэффициентов устойчивости на основе резервного ресурса логического и физического пространства состояний

| Количество физических резервных направлений | Количество логических резервных направлений | Количество допустимых физических резервных направлений | Количество допустимых логических резервных направлений | Коэффициент устойчивости | Коэффициент живучести |
|---|---|---|---|---|---|
| $F_{факт}$ | $L_{факт}$ | $F_{доп}$ | $L_{доп}$ | $K_{stab} = \frac{L_{факт}}{L_{доп}}$ | $K_{surv} = \frac{F_{факт}}{F_{доп}}$ |
| 2 | 2 | 6 | 10 | 0,2 | 0,33 |

Итоговый расчет защищенности, как без учета резервирования, так и с учетом резервирования представлен в таблице 4.

Таблица 4 – Оценка коэффициентов защищенности с учетом устойчивости, живучести на основе комплексной интегрированной модели оценки защищенности

| Коэффициент защищенности | Коэффициент защищенности с учетом устойчивости и живучести |
|---|---|
| $K_n^{ИБ}$ | $K_n^{Конф,КИ,N} = \frac{\left(\sum_{i=1}^{n} K_i^{КИ} + \sum_{i=1}^{n} K_i^{Конф}\right)}{\sum_{i=1}^{n}(K_n^{КИ} + K_n^{Конф} + K_n^{N})} K_{stab} + \frac{\sum_{i=1}^{n} N_i}{\sum_{i=1}^{n}(K_n^{КИ} + K_n^{Конф} + K_n^{N})} K_{sur}$ |
| $K_n^{ИБ} = 40 / 50 = 0.$ | $K_n^{Конф,КИ,N} = 40 / 50 \cdot 0,2 + 10 / 50 \cdot 0,33 = 0,8 \cdot 0,2 + 0,2 \cdot 0,33 = 0.226$ |

Для заданных исходных данных, определяемых параметрами коммуникационной инфраструктуры, получены точные оценки защищенности объекта КИИ. Для полученных оценок очевидны причинно-следственные связи защищенности объекта КИИ с параметрическими недостатками средств обеспечения информационной безопасности и направлением дальнейшего совершенствования политики информационной безопасности. В случае обеспечения функционирования объекта КИИ

в условиях компьютерных атак появляются как теоретические предположения, объясняющее этот процесс и поведение объекта КИИ в дальнейшем, так и практическое подтверждения для расчета оценок его защищённости.

**Заключение**

Таким образом, моделирование фрагментов КИИ (ИС, АСУТП, ИТС) на основе математического аппарата вложенных раскрашенных сетей Петри позволяет развивать элементы теории информационной безопасности в области моделирования и оценки защищенности объектов КИИ с учетом ее устойчивости в условиях воздействия КА. Моделирование на основе сетей Петри позволяет исследовать протокольные особенности построения объектов КИИ (ИС, АСУТП, ИТС) на свойства информационной безопасности, связанные с устойчивостью КИИ, доступностью, оценивать защищенность объектов. Формирование параметрических точных имитационных моделей КИИ позволяет строить цифровые двойники объектов коммуникационной инфраструктуры и в динамике исследовать функционирование таких объектов с учетом изменения конфигурации, воздействия нарушителя, формирования физических или логических резервных направлений связи. Полученные результаты позволяют получать количественные показатели оценки защищенности и устойчивости функционирования объектов КИИ в условиях воздействия нарушителя, исследовать влияние различных типов компьютерных атак на объекты КИИ.

## Литература


1. РосТелекомм. Аналитиечкий отчет об атаках на онлайн ресурсы компании за 2022 г. [сайт]. URL: https:// https://rt-solar.ru/upload/iblock/34a/5w4h9o57axovdbv3ng 7givrz271ykir3/Ataki-na-onlayn_resursy-rossiyskikh-kompaniy-v-2022-godu.pdf (дата обращения: 16.06.2023).
2. ТрансТелеКом. Аналитический отчет по сервису "Защита от DDoS-атак" за 1 квартал 2023 г. [сайт]. URL: https://ttk.ru/upload/doc/business/ddos_1_2023.pdf (дата обращения: 16.06.2023).
3. Бюллетени НКЦКИ: новые уязвимости ПО [сайт]. URL: https://safe-surf.ru/specialists/bulletins-nkcki/ (дата обращения: 01.11.2023).
4. 4. О безопасности Критической информационной инфраструктуры Российской Федерации: Федеральный закон ред. от. 19.07.2017г. №187 // ФСТЭК: [сайт]. – URL: https://fstec.ru/component/attachments/download/1906/. (дата обращения 27.02.2023).
5. **Петренко С.А.** Киберустойчивость цифровой индустрии 4.0: научная монография / С. А. Петренко. – Санкт-Петербург: Издательский Дом «Афина», 2020, – 256 с.
6. **Петренко С.А.** Киберустойчивость цифровой экономики. Как обеспечить безопасность и непрерывность бизнеса \ С. А. Петренко. – Санкт-Петербург: Издательство Прогресс книга, 2021. – 384 с. ISBN 978-5-4461-1763-5.
7. **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. – 500 с. ISBN 978-5-9912-0827-7.
8. **Величко В.В.** Модели и методы повышения живучести современных систем связи / В. В. Величко, Попков, . В., В. К. Попков. – Москва : Горячая линия – Телеком, 2017.–270 с. ISBN 978-5-94876-090-2.