DOI 10.36622/VSTU.2023.26.1.008
УДК 004.735

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ПОСТРОЕННЫХ НА БАЗЕ ПРОТОКОЛА BGP: АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОЦЕНКИ И РЕГУЛИРОВАНИЯ РИСКОВ РЕАЛИЗАЦИИ АТАКИ IP-HIJACKING

К.А. Разинкин, А.А. Науменко, А.И. Мордовин, О.Н. Чопоров, Ю.В. Макаров

В статье предложена методика повышения защищенности телекоммуникационных сетей, построенных на базе протокола BGP от атаки IP-hijacking, направленной на нарушение конфиденциальности и доступности перехваченной информации автономных систем. Ключевой составляющей данной методики является алгоритм оценки и регулирования рисков успешной реализации атаки IP-hijacking на телекоммуникационную сеть. В работе представлены особенности топологии телекоммуникационной сети, построенной на базе протокола BGP, и специфика атаки IP-hijacking, типовой сценарий реализации атаки, включающий описание уязвимостей сетевого оборудования, структура векторов и математическая оценка потенциала атаки IP-hijacking, также предложен инструментарий оценки и регулирования рисков. Полученные результаты в виде графика уровней риска позволяют определять область и возможные средства регулирования рисков сети, а также рассматривать возможный уровень ущерба конфиденциальности и доступности информации автономных систем.

Ключевые слова: протокол BGP, риск, атака IP-hijacking, конфиденциальность, телекоммуникационная сеть.

Введение

На современном этапе человеческой жизнедеятельности защита сетевого пространства является одной из первостепенных задач. В условиях трансформации мультисетевой среды специалистам в области обеспечения информационной безопасности намного чаще приходится решать вопросы, связанные с различными объектами и аспектами защиты информации: от интернета вещей [1] до контент-противоборства, от несанкционированного доступа [2] и до вирусных эпидемий [3]. Вместе с тем, недоисследованной остается область оценки и регулирования рисков успешной реализации атак IP-hijacking, эксплуатирующих уязвимости протокола BGP телекоммуникационных сетей. Значительную роль в этом противодействии играет инструментарий выявления уязвимостей и их риск-анализа.

Интернет представляет из себя телекоммуникационную сеть, включающую в себя великое множество взаимосвязанных небольших сетей, которые функционируют децентрализовано. Протокол маршрутизации BGP (Border Gateway Protocol) является ключевой технологией междоменной маршрутизации в сети Интернет, которая состоит из множества автономных систем (АС), находящихся под единой политикой маршрутизации.

Согласно обновленному Интернет-реестру CIDR, в мире насчитывается около 74080 автономных систем и 939050 возможных маршрутов распределения информации. Только в России, согласно статистике актуального сервиса IDIDB, зарегистрировано 5846 автономных систем [4-5]. Исходя из этого следует, что из-за линейного роста количества АС и расширения подключений между ними, увеличивается размер таблицы маршрутизации BGP, что является причиной больших проблем с масштабируемостью топологии сети Интернет.

К сожалению, как и множество сетевых протоколов, так и протокол BGP, проектировался до того, как интернет-пространство стало в большей степени небезопасно. Именно поэтому он разрабатывался без учёта значительных мер и

средств по защите передаваемой информации.

Компания Qrator Labs, специализирующаяся на защите информации, предоставила статистику о BGP-инцидентах в четвертом квартале 2021 года, в котором наблюдалось рекордное количество АС, пострадавших от утечек IP-маршрутов. Суммарное количество составило 17 799 автономных систем, подверженных реализации атаки IP-hijacking [6].

Атака IP-hijacking характеризуется деструктивным поведением, при котором неправильная настройка или перехваченное злоумышленником сетевое оборудование является причиной ложного маршрута к IP-префиксу. Введение ложного IP-префикса в протокол BGP также является одним из способов для перехвата и отслеживания трафика по пути к истинному маршрутизатору или для нарушения конфиденциальности и доступности передаваемой информации.

Главное противоречие в проблеме обеспечения информационной безопасности телекоммуникационных сетей, построенных на базе протокола BGP, заключается в разногласии темпов линейного роста топологии сети Интернет в условиях современного мира и устаревших средств защиты для предотвращения последствий сетевых атак, таких как IP-hijacking.

Риск-анализ защищаемых телекоммуникационных сетей является общепринятым алгоритмическим подходом к реализации системы мер и средств по обеспечению их безопасности, однако в существующих моделях и надстройках протокола BGP, являющихся аналогами, отсутствует описание механизма оценки рисков реализации атаки и правила их количественной оценки. Острой необходимостью является адаптация данных моделей безопасности для телекоммуникационных сетей, построенных на базе протокола BGP.

Исходя из вышеизложенного можно сделать вывод, что актуальность исследования характеризуется следующими факторами:

– стремительным ростом топологии сети Интернет за счёт линейного роста количества автономных систем и подключений между ними;

– высокой частотой эксплуатирования злоумышленниками уязвимостей протокола BGP при атаке IP-hijacking на телекоммуникационные сети;

– отсутствием должного уровня обеспечения защиты телекоммуникационных сетей, построенных на базе протокола BGP от атак, связанных с перехватом IP-префикса;

– недостаточной эффективностью инструментария у существующих аналогов, позволяющего провести оперативный риск-анализ объекта исследования.

Анализ аналогов оценки и регулирования рисков реализации атаки IP-hijacking

Методика обеспечения безопасности, построенная на оценке доверия в транспортных сетях VANET, описывает способ децентрализованного управления по обнаружению новых злонамеренных узлов интеллектуальной транспортной сети. На основе прямой и косвенной оценки доверия методика позволяет определить диапазоны рисков деструктивного поведения узлов сети. Однако, данный способ не определяет меры регулирования рисков из-за отсутствия специфики реализации атаки IP-hijacking. Также, к минусам можно отнести то, что корреляционный анализ, используемый в методике, не позволяет прогнозировать возможный размер ущерба при успешной реализации сетевых атак [7].

Метод ITSRA 1.0 (Information Technology Sector Baseline Risk Assessment – Базовая оценка рисков сектора информационных технологий) описывает комплексный подход к оценке и регулированию рисков Интернет-маршрутизации, сочетающий качественные методики анализа. ITSRA 1.0 сопоставляет меры регулирования рисков с конкретными сигнатурами, чтобы повысить степень безопасности ключевых объектов КИИ [8]. Оценка риска осуществляется по двум факторам: вероятность реализации и размер последствий (ущерба), что является базовой оценкой, в которой не учитывается количественная оценка риска и специфические особенности реализации атак

на телекоммуникационные сети, построенные на базе протокола BGP.

Политика защитной фильтрации потенциально опасных маршрутов BGP применяется для обнаружения и удаления вредоносных и потенциально деструктивных маршрутных объявлений, а также для регулирования потенциально опасных атрибутов полученных IP-префиксов. Сетевое оборудование тщательно отфильтровывает исходящие и входящие маршруты благодаря политикам маршрутизации. Именно поэтому, они являются эффективной и используемой мерой регулирования рисков безопасности протокола BGP [9]. Однако, неправильное конфигурирование защитной фильтрации на маршрутизирующем устройстве позволит злоумышленникам с большей вероятностью наносить ущерб автономным системам. Применительно к тематике данного исследования, эксплуатация политик защитной фильтрации не предусматривает комплексный риск-анализ реализации сетевых атак.

Методика обнаружения атаки IP-hijacking, построенная на многомерном анализе данных является эффективным средством установления надежного сопоставления между IP-префиксом и автономной системой с использованием общедоступных многомерных данных. На основании глубокого анализа данных методика позволяет количественно оценить риск реализации атаки за счет достоверности всех измерений, чтобы принять сопоставление происхождения AC и IP-префикса [10]. Однако, данный способ применим в сетях с высокими вычислительными возможностями, так как используется поэтапный алгоритм обнаружения атаки, что является весомым недостатком.

Описание методики математической оценки потенциала атаки IP-hijacking

Для эффективного проведения риск-анализа реализации атаки необходимо наиболее достоверно смоделировать возможные сценарии реализации угроз с учётом специфики протокола BGP.

Существует множество целей реализации перехвата IP-префикса злоумышленником, но ключевыми из них являются:

1. Перехват трафика других AC (обозначение – TL). При реализации атаки IP-hijacking в таблицы маршрутизации автономных систем добавляются существующие маршруты. Согласно межсетевому взаимодействию сетевых протоколов, будет выбран оптимальный маршрут, который анонсировал злоумышленник. Вся информация, которая соответствует пулу адресов перехваченного префикса, будет направляться на маршрутизатор злоумышленника.

2. Отказ сетевого оборудования в обслуживании сети (обозначение – DoS). На основании анализа сетевого сервиса BGPStream, позволяющего получить оповещения о перехватах IP-префикса, утечках информации и сбоях междоменной маршрутизации в сети Интернет, можно сделать вывод, что при реализации атаки IP-hijacking количество блоков адресов может варьироваться от нескольких десятков до нескольких тысяч. Не каждое скомпрометированное сетевое устройство может выдержать такой поток трафика. Вследствие чего, оборудование выходит из строя.

Однако, для успешного перехвата IP-префиксов злоумышленнику необходимо получить доступ к интерфейсу (CLI – Command Line Interface) маршрутизирующего оборудования атакуемой автономной системы посредством эксплуатации уязвимостей. Таким образом, подробное изучение отчётов компаний, специализирующихся на защите информации, позволило выделить приоритетный сценарий атаки IP-hijacking. Каждый элемент сценария включает в себя методы реализации:

1. Исследование топологии атакуемой сети:

- подробный анализ сервисов и Интернет-реестров префиксов и AC;
- социальная инженерия.

2. Удаленный доступ к CLI посредством эксплуатации уязвимостей сетевого оборудования:

• эксплуатация открытых портов сетевых устройств (обозначение – ONP);

• уязвимость, позволяющая выполнить произвольный код (обозначение – RCE);

• уязвимость, позволяющая повысить привилегии до уровня администратора (обозначение – EPE).

3. Реализация атаки IP-hijacking:

• объявление нового IP-префикса, который не принадлежит данной АС (обозначение – NP);

• объявление более конкретного IP-префикса (обозначение – SP).

Вышеизложенная моделируемая совокупность действий является сценарием реализации атаки, причем это один из множества сценариев, которые могут спровоцировать подобный инцидент. Каждый этап сценария обосновывает определенное воздействие, которое приближает злоумышленника к цели. Однако, каждый из этих этапов по отдельности не представляет угрозы для сети, а большая часть из них не может быть реализуема без выполнения начальных элементов сценария. Таким образом, моделирование сценария атаки позволяет оценить возможности злоумышленника.

Таким образом, для полного понимания сценария реализации атаки IP-hijacking и точного определения уровня опасности необходимо понимать основные принципы реализации уязвимостей второго и третьего этапа сценария. Применительно к тематике текущего исследования, методы реализации уязвимостей первого этапа сценария рассматриваться не будут, так как они основываются на специфике и личном мотиве злоумышленника.

В роли инструмента анализа уязвимостей сетевого оборудования выступает банк данных уязвимостей и угроз Федеральной службы по техническому и экспортному контролю (БДУ ФСТЭК России).

Таким образом, для дальнейшей математической оценки потенциала атаки IP-hijacking необходимо определить сложность доступа злоумышленника к интерфейсу сетевого оборудования для второго этапа сценария. Сложность доступа определяется качественной и количественной оценкой, изложенной в БДУ ФСТЭК России, по методике CVSS v2.0.

Для третьего этапа сценария необходимо оценить сложность реализации атаки IP-hijacking злоумышленником. Данный параметр характеризуется количественной оценкой включения атрибутов противодействия атаке в конфигурацию маршрутизирующего устройства. Таким образом, чем больше данных атрибутов включено в сетевое оборудование, тем выше оценка сложности реализации атаки IP-hijacking.

Очевидно, что вектором атаки в данном исследовании является совокупность методов реализации атаки на каждом этапе возможного сценария. При формализации данных параметров получим структуру вероятных векторов реализации атаки IP-hijacking на телекоммуникационные сети. Структура вероятных векторов реализации атаки IP-hijacking представлена в табл. 1.

Таблица 1

Структура вероятных векторов реализации атаки IP-hijacking

Вектор атаки первого этапа сценария	Вектор атаки второго этапа сценария	Вероятные цели атаки
ONP	NP	TL, DoS
	SP	
RCE	NP	TL, DoS
	SP	
EPE	NP	TL, DoS
	SP	

Для дальнейшей математической оценки потенциала атаки IP-hijacking будем

использовать структуру «вектор атаки 1 этапа сценария – вектор атаки 2 этапа сценария – цель атаки».

Понятие потенциала атаки вводится как показатель, характеризующий возможности по нанесению деструктивных последствий от реализации атаки, т. е. через риск нанесения ущерба автономным системам. Математическая оценка потенциала атаки осуществляется на основании параметров и характеристик элементов безопасности и уязвимостей сетевого оборудования.

Применительно к тематике данного исследования, потенциал атаки IP-hijacking будет оцениваться с учётом статического и динамического режима.

Схема концепции методики математической оценки потенциала атаки IP-hijacking представлена на рис. 1.

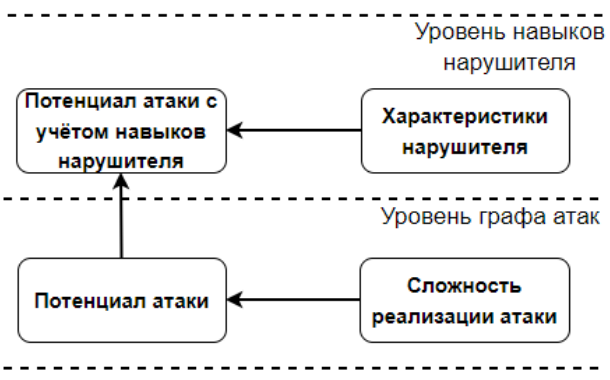

Рис. 1. Схема оценки потенциала атаки IP-hijacking

Методика оценки потенциала атаки IP-hijacking на основе вышеизложенной схемы включает в себя следующие этапы:

1. Каждая итерация является методом реализации атаки, с учётом его событий безопасности.

2. Очевидной стала необходимость введения метрики, демонстрирующей уровень навыков нарушителя. С помощью метода ранжирования определяется количественная оценка уровня навыков нарушителя (K_S):

– высокий уровень навыков, значение оценки находится в промежутке [0.72; 0.99];

– средний уровень навыков, значение оценки находится в промежутке [0.4; 0.71];

– низкий уровень навыков, значение оценки находится в промежутке [0.15; 0.39].

3. Вероятность реализации атаки от одного узла сети к другому обуславливается максимальной сложностью получения доступа к CLI, а также количественной оценкой включения атрибутов противодействия атаке в конфигурацию маршрутизирующего устройства при всех итерациях. Количественные оценки включения атрибутов безопасности (K_H) ранжируются на основе эффективности противодействия атаке IP-hijacking:

– инфраструктура ресурсов открытого ключа (RPKI), значение оценки составляет 0.54;

– префиксная фильтрация, значение оценки составляет 0.31;

– парольная аутентификация, значение оценки составляет 0.14.

Оценка сложности реализации атаки IP-hijacking вычисляется по формуле (1):

$$AC_{hijack} = 1 - \sum_{k=1}^{k} (K_H)_k \qquad (1)$$

где AC_{hijack} - сложность реализации атаки IP-hijacking;

$\sum_{k=1}^{k} (K_H)_k, k = \overline{1,3}$ - сумма количественных оценок атрибутов противодействия атаке.

Для объективной оценки потенциала атаки, необходимо с помощью методики CVSS v2.0 количественно оценить сложность получения доступа к CLI. На основании информации, опубликованной в БДУ ФСТЭК России, рассматриваемые уязвимости сетевого оборудования были расположены в порядке убывания сложности их эксплуатации, следовательно, и в порядке убывания эксплуатации векторов атак.

Ранжирование количественной оценки сложности получения доступа к интерфейсу маршрутизатора (K_{AC}) имеет следующий вид:

– уязвимая конфигурация сетевого оборудования встречается на практике очень редко (высокий), значение оценки составляет 0.35;

– затрагиваемая конфигурация отличается от конфигурации по умолчанию и обычно не настраивается (средний), значение оценки составляет 0.61;

– затронута конфигурация по умолчанию или вездесущая (низкий), значение оценки составляет 0.71.

4. На основе вышеописанных метрик определяются локальные безусловные вероятности для каждого вектора атаки.

5. Как описывалось выше, каждый из этапов сценария по отдельности не представляет большой угрозы для сети. Именно поэтому, успешность наступления второго этапа сценария (реализация атаки IP-hijacking) зависит от успеха первого этапа сценария (Удаленный доступ к CLI посредством эксплуатации уязвимостей сетевого оборудования). В конечном счёте, потенциал атаки на уровне графа атак определяется по формуле (2):

$$Pt_i = P(AB)_i = P(A)_i \times P(B/A)_i, \qquad (2)$$

где $P(A)_i$ - вероятность наступления первого этапа сценария;

$P(B/A)_i$ - условная вероятность наступления второго этапа сценария, при условии, что первый был успешно реализован;

i - вектор атаки IP-hijacking.

6. На втором уровне методики потенциал атаки IP-hijacking переопределяется с учётом оценки уровня навыков нарушителя по формуле (3):

$$Pt'_i = K_S \times Pt_i, \qquad (3)$$

где Pt'_i - потенциал атаки IP-hijacking с учётом оценки уровня навыков нарушителя для каждой итерации;

Pt_i - потенциал атаки уровня графа атак;

i - вектор атаки IP-hijacking;

K_S - коэффициент уровня навыков нарушителя.

Модель оценки и регулирования рисков реализации атаки IP-hijacking

Очевидной стала необходимость разработки математической модели оценки и регулирования рисков для возможных комбинаций векторов реализации атаки IP-hijacking, изложенных в табл. 1.

Для дальнейшего проектирования модели были выбраны и обоснованы следующие метрики оценки рисков успешной реализации атаки перехвата IP-префикса, каждая из которых будет использоваться в виде числового коэффициента:

– показатель потенциала атаки IP-hijacking (Pt');

– уровень ущерба конфиденциальности перехваченной информации автономной системы (K_C);

– уровень ущерба доступности информации автономной системы (K_A).

Количественный показатель потенциала атаки на основе уровней графа атак и навыков нарушителя (Pt') характеризуется как условная вероятность реализации атаки при определенном векторе.

Для определения значений метрик K_C и K_A, характеризующий вероятный уровень ущерба, возможные цели атаки были проранжированы в порядке убывания ущерба, который способна нанести успешная атака IP-hijacking телекоммуникационной сети, построенной на базе протокола BGP, достигнув поставленной цели. В табл. 2 показаны качественные и количественные оценки значений данных коэффициентов:

Таблица 2

Значения коэффициентов K_C и K_A для целей атаки

Цель атаки	K_C		K_A	
	Качеств.	Количеств.	Качеств.	Количеств.
TL	Высокий	0.078	Средний	0.053
DoS	Низкий	0.029	Высокий	0.078

Для регулирования рисков реализации атаки необходимо добавить метрику, отражающую эффективность средств противодействия атаке, способных минимизировать потенциал атаки, тем самым уменьшить значение ущерба АС при успешной реализации атаки. Качественная и количественная оценка уровня эффективности средств противодействия атаке ($K_{REACTION}$) имеют следующий вид:

- высокая эффективность средства, значение оценки составляет 1.9;
- средняя эффективность средства, значение оценки составляет 1.6;
- низкая эффективность средства, значение оценки составляет 1.1;
- средство противодействия отсутствует, значение оценки составляет 1.

Модель включает в себя общепринятую формулу расчёта рисков информационной безопасности, параметры которой переопределены на основе вышеизложенных метрик оценки рисков успешной реализации атаки перехвата IP-префикса. Формула расчёта рисков ИБ (4) без переопределения имеет вид:

$$risk = p(U) \times U, \quad (4)$$

где $p(U)$ - вероятность наступления ущерба определённой величины при реализации атаки;

U - величина вероятного ущерба.

При расчёте вероятности наступления ущерба для многокомпонентной телекоммуникационной сети, состоящей из множества автономных систем, необходимо учитывать вероятность реализаций атаки IP-hijacking на основе статистических данных. Подробно изучив статистику [11], можно сделать вывод, что реализации атаки представляют собой определенное число событий безопасности, произошедших за определенный промежуток времени (сутки), при том все события, независимо друг от друга, происходят с некоторой средней интенсивностью.

Данные свойства описывают простейший поток реализаций атаки IP-hijacking. Однако, при реальной топологии условия потока соблюдаются не постоянно. Процесс может быть нестационарен, т. к. в разное время или различные месяцы поток реализаций атаки может меняться, он может быть гораздо интенсивнее в периоды политической нестабильности. Но, в целом закон распределения Пуассона с хорошей степенью точности отражает многие процессы, следовательно, применим для использования при распределении вероятностей реализации атаки IP-hijacking [12].

Количество реализаций атаки IP-hijacking на телекоммуникационную сеть за интересующий нас интервал времени, назовем интенсивностью реализаций атаки и определим следующим образом: $\lambda = t/t_{\text{ср}}$, где $t_{\text{ср}}$ – среднее значение временного интервала между реализациями атаки [12].

Таким образом, для определения вероятности реализации атаки IP-hijacking целесообразно применять формулу распределения Пуассона (5), учитывающую длину выбранного интервала *t*:

$$p_k = \frac{(\lambda t)^k}{k!} e^{-\lambda t}, \quad (5)$$

где k – число реализаций атаки IP-hijacking;

λ - интенсивность, среднее число реализаций атаки за интервал времени t.

Но если, ввести величину $\lambda = \lambda t$, то формулу (5) можно упростить.

Вышеизложенная формула распределения Пуассона (5) указывает на постоянную реализацию k атак возникающих с интенсивностью λ. Однако, для текущей ситуации необходимо учитывать показатель потенциала атаки IP-hijacking (Pt'), характеризующийся как вероятность реализации атаки для определенного вектора.

Таким образом, перерасчёт вероятности реализации атаки IP-hijacking является равносильным перемножению полученной интенсивности реализаций атаки λ_i для определенного вектора на потенциал атаки Pt'_i. Формула вероятности реализации k атак IP-hijacking при заданной интенсивности λ_i с учётом потенциала атаки выглядит следующим образом:

$$p_k(Pt'_i, \lambda_i) = \frac{Pt'_i \lambda_i^k}{k!} e^{-Pt'_i \lambda_i}, \quad (6)$$

где λ_i – интенсивность реализации атаки для определенного вектора;

Pt'_i – показатель потенциала атаки IP-hijacking для определенного вектора;

k – количество реализаций атаки.

Как описывалось выше, при расчёте вероятности наступления ущерба для телекоммуникационной сети, состоящей из множества автономных систем, необходимо учитывать вероятность реализаций атаки IP-hijacking. Зная формулу вероятности реализации K атак IP-hijacking (6), возможно перейти к выражению для ущерба.

Предположим, что реализация атаки IP-hijacking для определенного вектора влечет за собой одинаковый ущерб ${U_h}^0$ автономным системам, тогда общий ущерб U_h при реализации k атак IP-hijacking определяется выражением: $U_h = k * {U_h}^0$. Для того, чтобы перейти к распределению вероятностей нанесения ущерба при реализации k атак определенного вектора, необходимо данное выражение подставить в формулу (6):

$$p_{U_h}(U_h) = \frac{Pt'_i \, \lambda_i^{(U_h / {U^0}_h)}}{(U_h / {U^0}_h)!} \mathrm{e}^{-Pt'_i \lambda_i}. \qquad (7)$$

Однако, для учёта различия величин ущерба от различных векторов реализации атаки IP-hijacking для оценки риска необходимо привести модель к общей шкале ущерба. Данный этап осуществим только для каждого из определенных векторов атаки в отдельности, поскольку величины ущербов как минимум, должны быть сопоставимыми и иметь одинаковую размерность.

При возникновении k реализаций атаки IP-hijacking, средний ущерб, наносимый автономной системе, равен $k * {U_h}^0$, а вероятность его нанесения равна p_{U_h}.

Таким образом, вероятность наступления ущерба определённой величины при реализации атаки IP-hijacking определенного вектора находится по формуле (7). Для расчёта риска наступления ущерба при реализации атаки также необходимо определить величину вероятного ущерба.

Величину вероятного ущерба (${U_h}^0$) от реализации атаки перехвата IP-префикса, для достижения конкретной цели (перехват трафика других АС (обозначение – TL) или отказ сетевого оборудования в обслуживании сети (обозначение – DoS)), необходимо считать, как сумму значений коэффициентов K_C и K_A для каждой автономной системы (8):

$$U^0{}_h = \sum_1^i (K_C + K_A)_i, i = 1...n, \qquad (8)$$

где K_C – уровень ущерба конфиденциальности перехваченной информации автономной системы;

K_A – уровень ущерба доступности информации автономной системы;

n – количество затронутых АС при реализации атаки.

Таким образом, применив полученные преобразования (6 – 7) к формуле (4), будет получена модель оценки рисков реализации атаки IP-hijacking (9), направленной на один из возможных векторов атаки, указанных в табл. 1 (например, «ONP – SP – TL») в телекоммуникационной сети:

$$Risk = p_{U_h}(U_h) \times U^0{}_{hi} = \frac{Pt'_i \, \lambda_i^{(U_h / U^0{}_{hi})}}{(U_h / U^0{}_{hi})!} \mathrm{e}^{-Pt'_i \lambda_i} \times U^0{}_{hi}, i = 1...n, \qquad (9)$$

где λ_i - интенсивность реализации атаки для определенного вектора;

U_h - общий ущерб при реализации k атак IP-hijacking, $U_h / {U_h}^0 = k$;

$U^0{}_{hi}$ - ущерб при реализации атаки IP-hijacking для определенного вектора;

Pt'_i - показатель потенциала атаки IP-hijacking для определенного вектора.

Подробное изучение отчётов компаний, специализирующихся на защите BGP сетей, позволило сделать вывод о том, что для снижения уровня риска реализации атаки IP-hijacking специалисты применяют специальные меры и средства по

противодействию, эффективность которых обоснована на реальном опыте [13].

Задача регулирования состоит в том, чтобы подобрать значения параметров, отвечающих за эффективность средств противодействия таким образом, чтобы в заданном диапазоне ущербов значения риска не превышали допустимого уровня. Однако, необходимо учитывать параметры системы, регулировкой которых можно целенаправленно управлять множеством параметров распределения. Как описывалось выше, от показателя потенциала атаки IP-hijacking (Pt'_i) зависит интенсивность реализации атаки (λ_i), тем самым изменяется количество реализаций атаки (k), что приводит к изменению вероятности наступления ущерба определённой величины при реализации атаки IP-hijacking ($p_{U_h}(U_h)$).

Таким образом, для регулирования полученного риска реализации атаки IP-hijacking в текущей модели можно обоснованно применить коэффициент эффективности средств противодействия ($K_{Reaction}$) к показателю потенциала атаки (Pt'_i). Для минимизации риска необходимо показатель потенциала атаки поделить на коэффициент эффективности средств противодействия ($Pt'_i \,/\, K_{Reaction}$).

Ключевым свойством коэффициента $K_{Reaction}$ является то, что при отсутствии средств противодействия в телекоммуникационной сети $\sum_{i=1}^{I} K_{Reaction} = 1$, так как в таком случае эффективность данных средств не влияет на уровень риска реализации атаки IP-hijacking.

Для подтверждения достоверности вышеизложенной модели построим график для вектора атаки «EPE – SP – DoS» (рис. 2) со следующими метриками:

1. интенсивность реализации атаки λ_i = 8 (согласно статистике BGPStream);

2. количество АС, понёсшие ущерб при реализации атаки составляет 10;

3. ущерб при реализации атаки определяется в соответствии с табл. 2 для цели DoS;

4. для регулирования рисков реализации атаки используется средство противодействия с коэффициентом 1.9.

Исходя из представленного графика можно сделать вывод, что потенциал атаки IP-hijacking играет ключевую роль. Чем выше потенциал, тем выше величина вероятного ущерба при реализации атаки. Если обратить внимание на огибающие рисков до регулирования и после, можно заметить, что при уменьшении рисков в одном диапазоне ущербов, неизбежно увеличивается риск в других диапазонах U. Это происходит осознанно, так как в критическом диапазоне ущербов возникает необходимость минимизации риска, а в незначительных диапазонах допускается рост риска, который неизбежен.

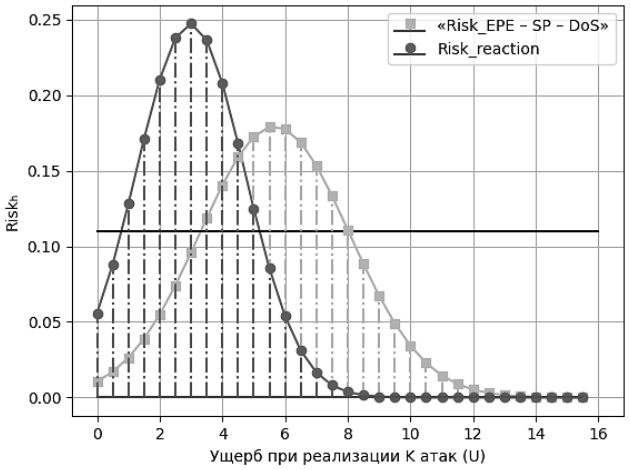

Рис. 2. Оценка и регулирование рисков для вектора «EPE – SP – DoS»

На основе огибающих риска, можно сделать вывод, что применение средств противодействия позволяет уменьшить риск нанесения вероятного ущерба при реализации атаки IP-hijacking в интервале существенного ущерба.

Данная модель оценки и регулирования рисков реализации атаки IP-hijacking будет служить основой при разработке алгоритмического и программного обеспечения необходимого регулирования рисков успешной реализации атаки.

Алгоритмическое обеспечение необходимой оценки и регулирования рисков реализации атаки IP-hijacking на телекоммуникационную сеть, построенную на базе протокола BGP

В контексте текущего исследования, предложенный программный алгоритм будет анализировать степень защищённости телекоммуникационной сети на примере

реальной конфигурации маршрутизирующего устройства с помощью вышеизложенной методики математической оценки потенциала атаки и модели оценки и регулирования рисков реализации атаки IP-hijacking.

Инструментарий на основе программного алгоритма может быть разработан с помощью языка программирования Python 3. Для реализации методики оценки потенциала и модели оценки и регулирования рисков, а также для визуальной составляющей рекомендуется использовать следующие библиотеки: PySimpleGUI, NumPy и Matplotlib.

Блок-схема алгоритма повышения защищенности телекоммуникационной сети от атаки перехвата IP-префикса, направленной на нарушение конфиденциальности и доступности перехваченной информации автономных систем представлена на рис. 3.

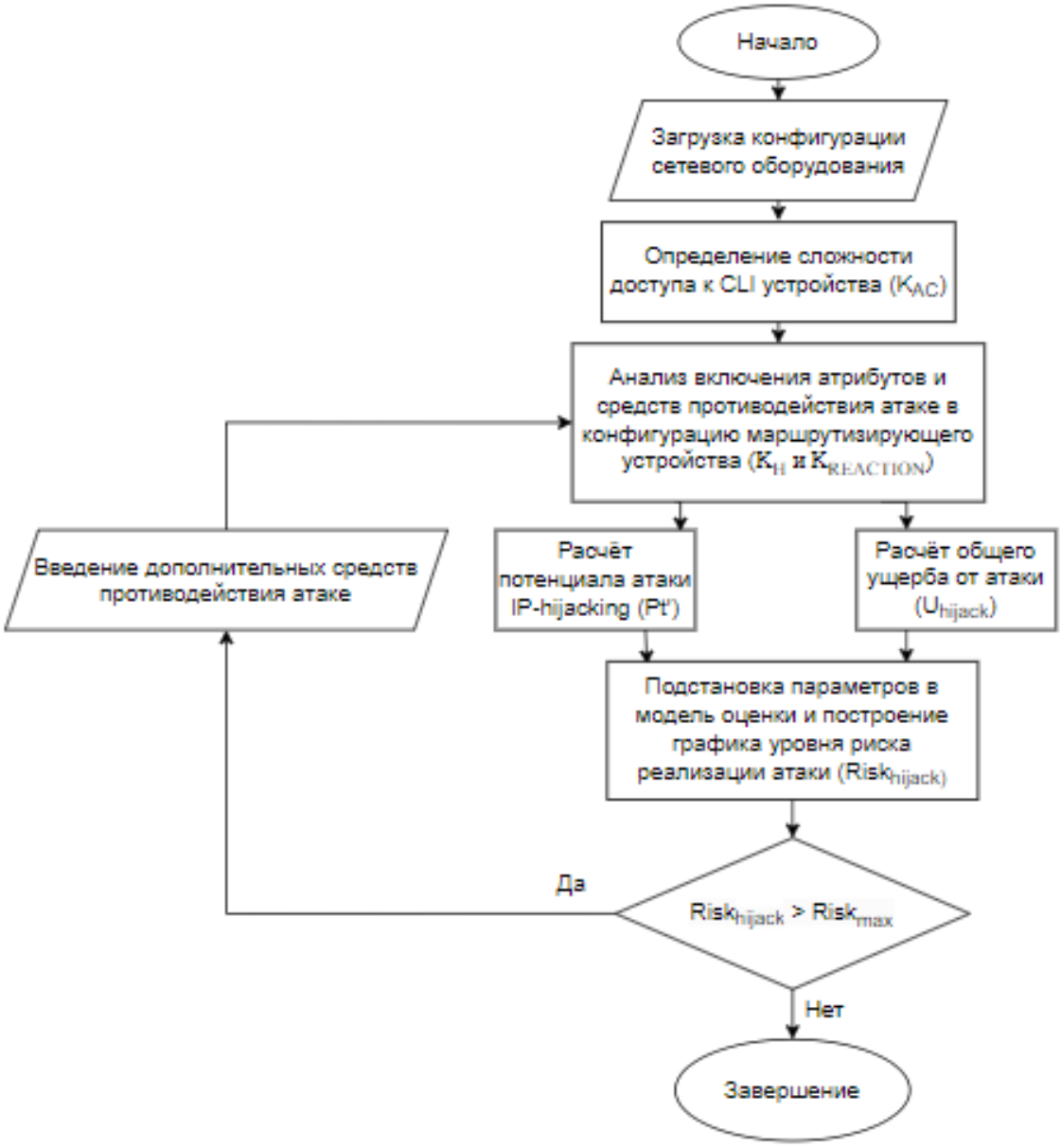

Рис. 3. Программный алгоритм оценки и регулирования рисков реализации атаки IP-hijacking

Заключение

Предложенная методика математической оценки потенциала атаки IP-hijacking позволяет производить вычисления с учётом топологии телекоммуникационной сети, построенной на базе протокола BGP.

Основным преимуществом разработанной модели оценки и регулирования рисков реализации атаки IP-

hijacking является ее способность построения графика уровня риска, что даёт возможность определения области регулирования рисков телекоммуникационной сети. Полученные графики позволяют сделать вывод о том, что применение средств противодействия позволяет уменьшить риск нанесения вероятного ущерба автономным системам при реализации атаки IP-hijacking в интервале существенного ущерба.

Программное обеспечение, разработанное на основе предложенного алгоритма оценки и регулирования рисков реализации атаки IP-hijacking, как компонент системы анализа защищенности, или как отдельный инструмент обеспечения информационной безопасности можно внедрить на уровне провайдера телекоммуникационных услуг.

Список литературы

1. Ермаков С.А. Оценка и регулирование рисков нарушения информационной безопасности телекоммуникационных сетей связи и управления промышленного интернета вещей. / С.А. Ермаков, Я.М. Каценко, А.А. Болгов, В.В. Сафронова, К.В. Сибирко. // Информация и безопасность. 2020. Т. 23. Вып. 1. С. 107-114.

2. Пахомова А.С. К вопросу о классификации автоматизированных систем в защищенном исполнении. / А.С. Пахомова, В.К. Власов, А.В. Паринов. // Информация и безопасность. 2019. Т. 22. Вып. 2. С. 272-275.

3. Остапенко А.Г. Математическое обеспечение комплекса моделирования эпидемических процессов с учетом дозировки вирусов: модель «Бахчисарайский фонтан». / А.Г. Остапенко, Е.А. Шварцкопф, А.А. Остапенко, В.В. Сафронова, К.В. Сибирко, Е.А. Болгова. // Информация и безопасность. 2021. Т. 24. Вып. 4. С. 553-560.

4. Интернет-реестр CIDR: сводка состояния таблиц BGP. URL: https://www.cidr-report.org/as2.0/ (дата обращения: 27.12.22).

5. Сервис IDIDB AS Рунета. – URL: https://www.ididb.ru/autnum/ (дата обращения: 27.12.22).

6. Статистика DDoS-атак и BGP-инцидентов в четвертом квартале 2021 года. URL: https://qrator.net/ru/company/news/statistika-ddos-atak-i-bgp-intcidentov-v-chetvertom-kvartale-2021-goda (дата обращения: 27.12.22).

7. Biswas. S. ID-based safety message authentication for security and trust in vehicular networks. / S Biswas, J Misic, V Misic. // Distributed Computing Systems Workshops (ICDCSW). 2011. P. 2-9.

8. Information Technology Sector Baseline Risk Assessment. URL: https://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf (дата обращения: 28.12.22).

9. Caesar M. BGP routing policies in ISP networks. / M. Caesar, J. Rexford // IEEE Network. 2005. Vol. 19. № 6. P. 5-11.

10. Zeng M. A BGP Hijacking Detection Method based on Multi-Dimensional Historical Data Analysis. / M. Zeng, H. Li, J. Lai, X. Huang // IEEE. International Conference on Computer Communication and Artificial Intelligence (CCAI). 2021. Vol. 10. P. 141-144.

11. BGPStream. URL: https://bgpstream.crosswork.cisco.com/ (дата обращения: 24.12.22).

12. Простейший поток. URL: https://infopedia.su/4x84fb.html (дата обращения: 24.12.22).

13. BGP Hijacking and BGP Security. URL: https://www.team-cymru.com/post/bgp-hijacking-and-bgp-security (дата обращения: 24.12.22).

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 27.12.2022

Информация об авторах

Разинкин Константин Александрович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: kostyr@mail.ru

Науменко Артём Александрович – студент, Воронежский государственный технический университет, e-mail: krazinkin@ccgeu.ru

Мордовин Андрей Иванович – старший преподаватель, Воронежский государственный технический университет, e-mail: krazinkin@ccgeu.ru

Чопоров Оллег Николаевич – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Макаров Юрий Вадимович – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

IMPROVING THE SECURITY OF TELECOMMUNICATION NETWORKS BUILT ON THE BASIS OF THE BGP PROTOCOL: ALGORITHMIC SUPPORT FOR THE ASSESSMENT AND REGULATION OF IMPLEMENTATION RISKS IP HIJACKING ATTACKS

K.A. Razinkin, A. A. Naumenko, A.I. Mordovin, O.N. Choporov, Yu.V. Makarov

The article proposes a method for improving the security of telecommunication networks built on the basis of the BGP protocol from an IP-hijacking attack aimed at violating the confidentiality and availability of intercepted information of autonomous systems. A key component of this methodology is an algorithm for assessing and managing the risks of a successful IP-hijacking attack on a telecommunications network. The article presents the features of the topology of a telecommunications network built on the basis of the BGP protocol and the specifics of the IP-hijacking attack, a typical scenario for the implementation of an attack, including a description of network equipment vulnerabilities, the structure of vectors and a mathematical assessment of the potential of an IP-hijacking attack, as well as a toolkit for risk assessment and management. The results obtained in a graph of risk levels make it possible to determine the scope and possible means of regulating network risks, as well as to consider the possible level of damage to the confidentiality and availability of information of autonomous systems.

Key words: BGP protocol, risk, IP-hijacking attacks, privacy, telecommunication network.

Submitted 27.12.2022

Information about the authors

Konstantin A. Razinkin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: kostyr@mail.ru

Artyom A. Naumenko – student, Voronezh State Technical University, e-mail: krazinkin@ccgeu.ru

Andrey I. Mordovin – senior lecturer, Voronezh State Technical University, e-mail: krazinkin@ccgeu.ru

Oleg N. Choporov – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: kostyr@mail.ru

Yurii V. Makarov – student, Voronezh State Technical University, e-mail: krazinkin@ccgeu.ru