Надежность, том 25, №4, 2025 / Dependability 4, 2025
Методы и системы защиты информации.
Информационная безопасность

УДК 004.056
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-4-43-51

Оценка защищенности от информационных атак на интеллектуальные транспортные системы с многоуровневой системой защиты информации

Evaluation of cyber security of intelligent transportation systems with a multi-level information protection system

Алексеев В.М.[1], Баранов Л.А.[1], Чичков С.Н.[1]*
Alekseev V.M.[1], Baranov L.A.[1], Chichkov S.N.[1]*

[1] Российский университет транспорта (МИИТ), Москва, Российская Федерация
[1] Russian University of Transport (MIIT), Moscow, Russian Federation
** seriozha.tchichkov@yandex.ru*

Алексеев В.М.

Баранов Л.А.

Чичков С.Н.

Резюме. **Цель.** *Рассмотреть вопросы оценки защищенности от информационных атак на интеллектуальные транспортные системы с многоуровневой системой защиты информации. С целью предотвращения атак, нацеленных на захват информации в многоуровневой системе защиты, предложено реализовать ядро локальной вычислительной сети (на всех уровнях) по полносвязной схеме. Это позволяет организовывать случайные доверенные маршруты, которые после выполнения функции по передаче информации разбираются, то есть ограничены по времени существования. Передача информации по случайно выбранным доверенным маршрутам с ограниченным временем существования затрудняет проведение внутренних атак с целью захвата объектов сети, по которым передается критически важная информация.* **Методы.** *В статье применяются методы математического анализа, теории графов и теории вероятностей.* **Результаты.** *Рассмотрена модель захвата трафика атакующим при выбранной защитником случайной стратегии формирования маршрутов в полносвязной сети. Проведена оценка модели защиты информации в многоуровневой системе защиты информации. Предложено при реализации многоуровневой системы защиты для предотвращения перехвата информационных потоков использовать динамически организуемые доверенные маршруты в условиях полносвязности.* **Заключение.** *Предложенная в статье методика позволяет оценить уменьшение вероятности захвата вершин полносвязной сети, а также оценить вероятность захвата вершин в зависимости от длительности передаваемого сообщения.*

Abstract. **Aim.** *To examine the assessment of cyber security of intelligent transportation systems with a multi-level information protection system. For the purpose of preventing attacks aimed at capturing information in a multi-level protection system, it is proposed to implement a fully connected core of the local area network (at all levels). This enables random trusted paths that are dismantled upon transmitting the information, i.e. are limited in their time of existence. Communicating information along randomly selected trusted limited-lifetime paths complicates internal attacks that aim to capture network entities involved in the communication of critical information.* **Methods.** *The paper uses methods of mathematical analysis, graph theory, and probability theory.* **Results.** *The authors examine a model of traffic capture by an attacker, whereas the defender uses random pathing in a fully connected network. A model of information protection in a multi-level information protection system was assessed. It is proposed using dynamically organised trusted paths in fully connected environments when designing a multi-level protection system to prevent interception of information flows.* **Conclusion.** *The proposed technique allows estimating the decrease in the probability of vertex capture in a fully connected network, as well assessing the probability of vertex capture depending on the duration of message transmission.*

Ключевые слова: *полносвязность, маршрут, вершина-объект, атакующий, защитник, виртуализация.*
Keywords: *full connectivity, path, vertex object, attacker, defender, virtualisation.*

Для цитирования: *Алексеев В.М., Баранов Л.А., Чичков С.Н. Оценка защищенности от информационных атак на интеллектуальные транспортные системы с многоуровневой системой защиты информации // Надежность. 2025. №4. С. 43-51. https://doi.org/10.21683/1729-2646-2025-25-4-43-51*

For citation: *Alekseev V.M., Baranov L.A., Chichkov S.N. Evaluation of cyber security of intelligent transportation systems with a multi-level information protection system. Dependability 2025;4: 43-51. https://doi.org/10.21683/1729-2646-2025-25-4-43-51*

Поступила: *02.06.2025* / **После доработки:** *11.07.2025* / **К печати:** *28.09.2025*
Received on: *02.06.2025* / **Revised on:** *11.07.2025* / **For printing:** *28.09.2025*

Введение

Защита информационных ресурсов требует совершенствования не только технических средств, но и разработки новых моделей идентификации атак, обеспечивающих защиту от внешних и внутренних угроз в локальных вычислительных сетях, а также создания принципов управления и программно-технической реализации сетевой инфраструктуры для систем различного назначения транспортного комплекса. Особенность сетей интеллектуальных транспортных систем заключается в том, что в них значительно возрастают объемы передаваемой информации с использованием маршрутизации информационных потоков, направляемых в центры обработки информации от различных источников. Центральной задачей интеллектуальных транспортных систем является обеспечение безопасной перевозки грузов и пассажиров. В этой связи обеспечение защиты сетевой инфраструктуры интеллектуальных транспортных систем (как критических объектов) является актуальной задачей.

Обеспечение защиты для критически важных объектов [1, 2, 3] предложено осуществить с использованием принципа многоуровневости. Реализация многоуровневой системы базируется на разделении функций, выполняемых на разных уровнях. Каждый из уровней нацелен на выполнение функций отражения внешних и внутренних атак путем использования анализаторов различных типов. В случае обнаружения атаки от внешних или внутренних источников анализаторы прерывают информационный поток, поскольку расположены посредине между источником и получателем. В статье предложено политику безопасности в многоуровневой

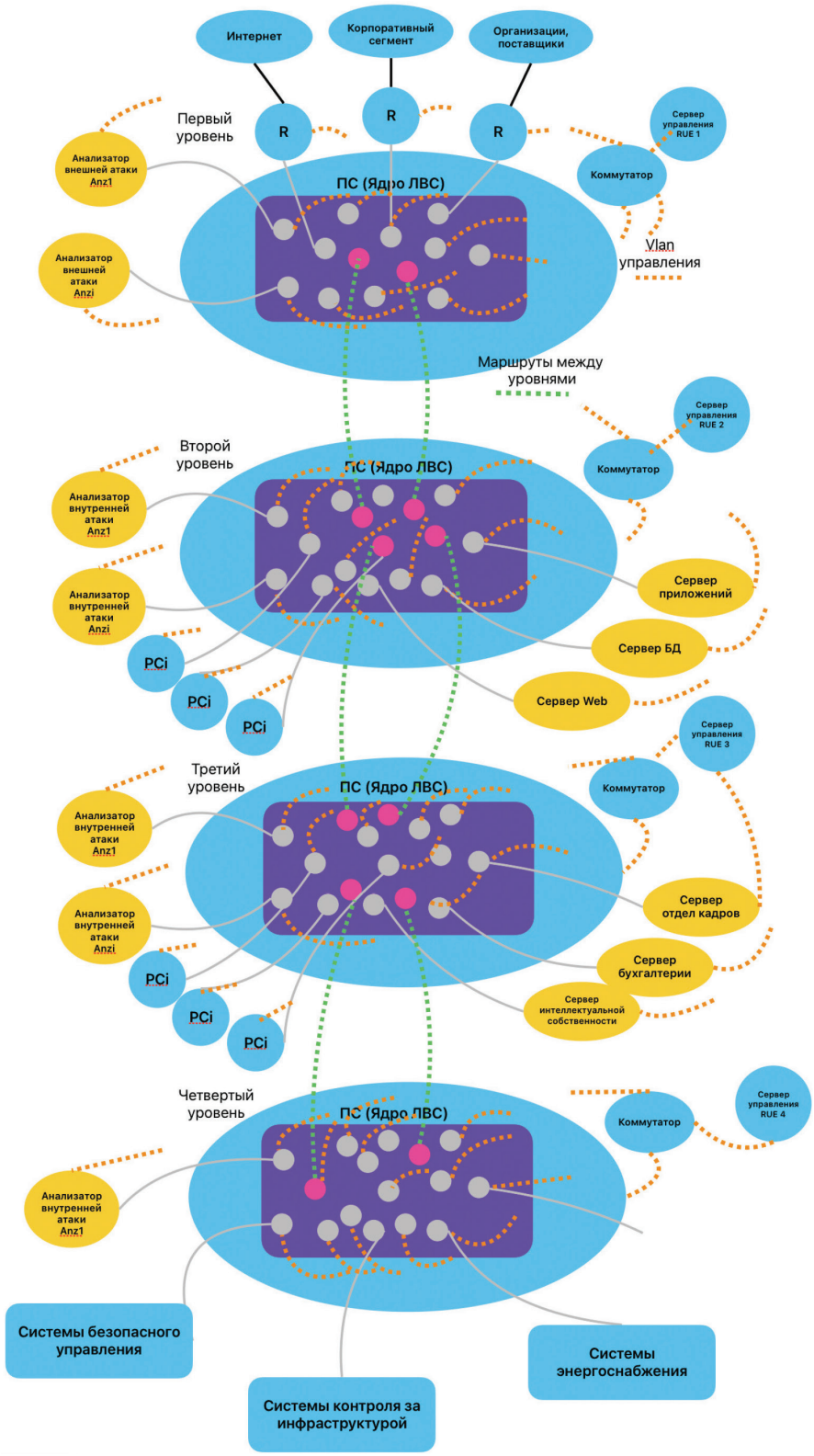

Рис. 1 Структура многоуровневой системы защиты информации

системе защиты строить на формировании случайных, динамически организуемых доверенных маршрутах, что позволяет защититься от внутренних атак перехвата информационных потоков.

Рассмотрена модель построения системы защиты информации, реализующей принцип «убегающего защитника от атакующего». Модель «убегающего защитника от атакующего» предложено реализовать на основе игры преследования на графах, где атакующий пытается получить доступ к объекту, включенному в маршрут передачи информации в текущий момент времени, а защитник формирует маршруты на графах (маршруты доставки информации в компьютерной системе). Задача атакующего (атакующих) – получить доступ к маршруту доставки информации в компьютерной системе, формируемому защитником (с целью получения конфиденциальной информации), а цель защитника – избегать захвата.

Цель исследования – оценить защиту информации в многоуровневой системе с динамически изменяемыми маршрутами. Для достижения цели необходимо решить следующие задачи:

- определить вероятность захвата вершины – объекта, включенного в случайно выбранный маршрут, по которому передается информационный поток;

- определить длительность захвата атакующим вершины – объекта, по которой передается информационный поток.

1. Функционирование многоуровневой модели защиты информации

На каждом уровне реализована полносвязная сеть (рис. 1). На первом уровне располагаются сетевые объекты локальной вычислительной сети, обеспечивающие связь с внешними корпоративными сетями, пользователями ресурсов и интернетом. С целью предотвращения возможных атак из внешних систем на первом уровне устанавливаются анализаторы *Anz*, каждый из которых нацелен на заданный тип информационной атаки *Inf*. На первом уровне нет персональных компьютеров субъектов и серверов.

Здесь происходит анализ трафика на присутствие внешних информационных атак. Сформированы признаки, на основании которых анализаторами *Anz* выявляются информационные атаки *Inf*. Передача информационных потоков из одного уровня в другой и обратно осуществляется в случае отсутствия признаков атак. На каждом уровне многоуровневой системы защиты локальная сеть реализована с использованием модели изолированной программной среды (ИПС) с использованием VLAN [4, 5, 6, 7]. Маршруты формируются сервером *RUE* [7,8]. Для реализации данной функции (формирования маршрутов *RUE*) создается отдельный *vlan–contr* управления. Сервер *RUE* формирует и отправляет конфигурационные файлы по *vlan–contr* на объекты, включаемые в маршрут (технология SDN (Software Defined Networking)) [8], где задается маршрут – vlan и политика информационного потока: порты, *vlan*, тип протокола, приоритетность, активность).

Маршруты на всех уровнях системы защиты реализуются также с помощью *vlan* с использованием серверов RUE_I, I=1,n. Объекты сети, не включенные в маршруты, неактивны. Маршрутизатор по маршруту, сформированному сервером *RUE*, направляет пакеты на *Anz* с тегом *vlan*, в котором определен протокол, приоритет и задан номер *vlan*. Передача информации из первого уровня во второй осуществляется по случайно заданным маршрутам, определяемым серверами RUE_I.

На втором уровне системы защиты располагаются субъекты с персональными компьютерами, сервера различных ресурсов (web, vks, mail, информационные базы для работы с клиентами и другие ресурсы).

На третьем уровне располагаются критически важные ресурсы, требующие усиленной защиты, такие как базы персональных данных, базы ноу-хау, бухгалтерии и другие ресурсы. Маршруты, связывающие второй уровень и третий, формируются также случайно серверами RUE_I, I=2,3.

На четвертом уровне защиты реализуются технологии, обеспечивающие функционирование систем безопасного управления на основе технологии мультисервисной передачи информации или других существующих технологий передачи информации, используемых для реализации интеллектуальных систем управления. Передача данных из третьего в четвертый уровень и наоборот также осуществляется по случайно заданным маршрутам RUE_I, I=3,4 .

На каждом уровне возможно появление внутренних атак, возникающих в результате неумышленных или злоумышленных действий субъектов. В этой связи, на каждом уровне устанавливаются анализаторы внутренних атак, основанные на использовании моделей профиля субъектов.

Рассмотрим граф $G=(V,E)$, описывающий состояние объектов локальной сети, расположенных на первом уровне, по которым передаются данные между объектами (маршрутизаторами и анализаторами *Anz*), где $V=\{v_1,v_2,\ldots,v_n\}$ – множество вершин – объектов локальной вычислительной сети, $E \subseteq V_i \times V_j; i, j = 1, n; i \neq j$ – множество ребер (обозначают связи между объектами). Объекты полносвязной сети $n_I \in n$ включены в общую сеть, где n_I – количество объектов в ядре ПС на уровне I. При этом, $n > n_I$, так как в n включаются персональные компьютеры, маршрутизаторы, собственно объекты ядра полносвязной ПС сети и другие объекты сетевой структуры.

Маршруты в ПС сети на каждом уровне I формируются специальным сервером управления RUE_I с использованием специальных протоколов (Open flow, rest api) [8, 9, 10, 11]. Маршруты $M_{k_i}^{RUE_I}$ простые и образуют множество, формируемое методом группового учета аргументов [12, 13], состоят из:

- наикратчайших маршрутов

$$M_{k_1}^{RUE_I} = V_i \times V_j; i, j = 1, n; i \neq j,$$

где k_1 – идентификатор наикратчайших маршрутов;

- маршрутов через один промежуточный объект

$$M_{k_2}^{RUE_I} = V_i \times V_k \times V_j; i, j, k = 1, n; i \neq \langle j, k \rangle; j \neq k,$$

где k_2 – идентификатор маршрутов с одним промежуточным объектом;

- маршрутов через два промежуточных объекта

$$M_{k_3}^{RUE_I} = V_i \times V_k \times V_l \times V_j; i, j, k, l = 1, n;$$
$$i \neq \langle j, k, l \rangle; j \neq \langle k, l \rangle; k \neq l,$$

где k_3 – идентификатор маршрутов с двумя промежуточными объектами;

- аналогично для маршрутов, проходящих через три и более промежуточных объектов.

Для всех маршрутов можно записать общую формулу:

$$\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I} = V_i \times V_j; \| V_i \times V_k \times V_j; \| V_i \times V_k \times V_l \times V_j;$$
$$\| \cdots_{i,j,k,l=1,n; i \neq \langle j,k,l \rangle; j \neq \langle k,l \rangle; k \neq l},$$

где n_1 – число промежуточных объектов в простых маршрутах, n_1=1,2,3,…h.

Рассмотрим формирование маршрутов передачи информации из первого во второй уровень. Информационные потоки поступают из внешней сети (корпоративный сегмент, либо интернет, либо пользователи юридические субъекты) на первый уровень многоуровневой системы защиты и маршрутизируются на анализаторы *Anz* внешних атак. Обозначим T – время существования маршрута $M_{k_i}^{RUE_I}$, которое складывается из времени формирования маршрута сервером RUE_I по команде от анализатора, пропуска трафика и далее завершения маршрута, то есть его разборки. Анализаторы на основе поступившей информации формируют признаки и принимают решение о запрете или пропуске трафика. Если *Anz* установлено, что в информационном потоке не содержится некорректной информации, *Anz* передает команду серверу RUE_I на конфигурацию маршрута. Информационный поток отправляется на второй уровень. В случае обнаружения *Anz* некорректной информации, маршрут для информационного потока запрещается. Обслуживание запросов от внешних пользователей осуществляется на втором уровне многоуровневой системы защиты, где располагаются основные ресурсы.

Трафик передается во второй уровень по маршруту, формируемому серверами RUE_1 и RUE_2 – первого и второго уровня. Индексы 1, 2 означают принадлежность к первому и второму уровням. Сервер RUE_1 назначает k_s объект, через который должен пройти маршрут передачи трафика из первого уровня во второй. Сервер RUE_1 сообщает RUE_2 об объекте k_s и под маршрут сервер RUE_2 выделяет k_s в ядре второго уровня защиты. Номер k_s выбирается из условия $k_s \neq \langle i, j, k_1 \ldots \rangle$ участвующих в организации маршрутов от маршрутизаторов к анализаторам на первом уровне. Маршрут описывается:

$$(V_i \times V_k \times V_{k_s})^{RUE_1} \times (V_{k_s} \times V_k \times V_i)^{RUE_2};$$
$$i, k_s, k = 1, n; i \neq \langle k_s, k \rangle; k_s \neq k.$$

Исходные условия задачи:

- граф содержит n вершин;
- атакующий A на каждом шаге j случайно выбирает одну вершину ядра ПС (равновероятно);
- защитник D прокладывает независимые, случайно выбранные маршруты с k_i промежуточными вершинами-объектами в ядре ПС;
- захват происходит, если хотя бы один маршрут защитника D проходит в той же вершине V_i, которую выбрал атакующий;
- движение атакующего A и защитника D происходит случайно и независимо друг от друга.

Рассмотрим внутреннюю атаку, которая может быть организована на втором, третьем или четвертом уровнях одиночным атакующим A на объекты ядра сети. (*Уязвимость CVE-2024-20399, CVE-2021-40119, оценивается на 9,8 из 10 по системе CVSS и является следствием несовершенства механизма аутентификации SSH в Cisco Policy Suite. Воспользовавшись этой уязвимостью, злоумышленник может подключиться к устройству по SSH, авторизовавшись как root)*.

Поскольку сеть полносвязная, то не все вершины-объекты активны, а только те, через которые проходят информационные потоки. Атакующий A пытается получить информацию путем овладения одной из вершин полносвязной сети, по которой проходит информационный поток, сформированный защитником D. Стратегию защитника D атакующий A не знает. Атакующий A движется равновероятно (случайное блуждание) по соседним вершинам. Состояние атакующего A обозначим $V_A(t)$ в момент времени t. Атакующий A может вставать на любую вершину – объект ПС сети с целью получить доступ к информационному потоку. Состояние защитника D в момент времени t представляется маршрутом $M_k(t) \in \bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}$. Маршрут $M_k(t)$ защитника D проходит по объектам, включенным в этот маршрут сервером управления RUE_I. Обозначим t_{M_k} – время существования маршрута. Если атакующий A, встав на вершину $V_A(t) \in M_k(t) \in \bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}$, по которой проходит маршрут информационного потока, овладевает им, то считаем, что атакующий A достиг цели.

Рассмотрим задачу определения вероятности захвата вершины – объекта, включенного в случайно выбранный маршрут, по которому передается информационный поток.

Решение. Защитник D формирует маршрут информационного потока, проходящий через вершины – объекты ядра ПС:

$$\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l} = V_i \times V_j; \left\| V_i \times V_k \times V_j; \right\| V_i \times V_k \times V_l \times V_j; \left\| \cdots_{i,j,k,l=1,n; i \neq \langle j,k,l \rangle; j \neq \langle k,l \rangle; k \neq l}. \quad (1)$$

Возможны два случая. Случай первый – маршрут информационного потока проходит через объект – вершину V_i, i=1,n принадлежащую одному из объектов, участвующих в формировании маршрута (1). A атакует вершину – объект V_i и получает доступ к информации в промежуток времени T существования информационного потока $\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l}$, проходящего через V_i, i=1,n , то есть $V_A(t) = \left(V_i \in M_k(t)\right) \in \bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l}$.

Случай второй – если информационный поток не проходит через объект – вершину V_i, i=1,n, то A не получает доступа к информационному потоку, то есть $V_A(t) = V_i \notin \bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l}$.

Оценку захвата вершины V_i атакующим A в полносвязной сети выполним с помощью параметра центральности вершины $C(V_i)$, который показывает связность (важность) вершины – объекта для формирования маршрутов передачи информационных потоков в сети и определяется:

$$C(V_i) = n_s \times \frac{P_{i,j}}{n_{sv}}, j = 1, n; n > 1, \quad (2)$$

где n_s – связи V_i вершины – объекта с соседними вершинами, равно n–1;

$P_{i,j}$ – вероятность осуществления передачи информации из вершины – объекта i к соседним вершинам – объектам, не занятым в маршруте;

n_{sv} – общее количество связей в ПС сети уровня I, n_{sv}=n×(n–1) (конечная вершина 0 граф n=1).

Примем вероятность перехода из вершины – объекта V_i к соседним объектам $P_{i,j}$=1/(n–1).

Защитник D выбирает случайную стратегию формирования маршрута $M_{k_i}^{RUE_l}$. В этом случае, вероятность выбора вершины – объекта V_i из всех вершин – объектов, задействованных в маршрутах $\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l}$, определяется как $P_{V_i}^d = \frac{n_{v_i}}{\sum_{k=1}^{n} \left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l} \right)}$.

Из формулы (1) следует (подставив значения n_s, n_{sv}, $P_{i,j}$), что для полносвязного ядра (для любого из уровней I) параметр центральности вершины для всех одинаковый и равен

$$C(V_i) = 1/\left(n \times (n-1)\right), j = 1, n. \quad (3)$$

При выборе стратегии случайного формирования маршрутов защитником D вероятность захвата информационного потока на вершине V_i атакующим A равна

$$P_{V_i} = C(V_i) \times P_{V_i}^d. \quad (4)$$

Наличие нескольких маршрутов в ядре изменяет величину $C(V_i)$, поскольку меняются параметры n_s и $P_{i,j}$ из-за уменьшения количества вершин, с которыми возможно организовать маршрут, что вытекает из ограничения соединения с соседней вершиной – объектом, занятым в маршруте (условие простого маршрута). Причем, при формировании маршрутов с промежуточными объектами параметр принимает значение равное

$$P_{i,j} = 1/\left((n-1)-k\right), \quad (5)$$

где k – соседние объекты, задействованные в маршрутах.

Из последней формулы (5) вытекает, что вероятность захвата информационного потока атакующим A возрастает при наличии действующих маршрутов в ядре ПС на любом из I-их уровней. Преодолеть возникшую коллизию возможно с использованием модели изолированной программной среды и виртуализации сети. Использование виртуализации позволяет формировать маршруты на портах объектов (на одном порту объекта можно организовывать несколько *vlan*), что позволяет формировать простые маршруты, проходящие одновременно по разным портам на одном объекте. Это позволяет исключить из формулы (4) переменную k.

Рассчитаем вероятность захвата атакующим A за время T вершины V_i, по которой передается информационный поток. Если атакующий движется случайным образом, то вероятность того, что вершина – объекта V_i в момент времени t будет занята A, равна:

$$P_{V_i}(T) = 1 - \prod_{t=1}^{T} \left(1 - p_i\left(x_D(t) = x_A^j(t)\right)\right), \quad (6)$$

где $p_i\left(x_D(t) = x_A^j(t)\right)$ – вероятность занятия V_i в момент времени t атакующим A, j=1,m – шаги по вершинам V_i сети.

Если атакующий движется равновероятно (случайное блуждание) по соседним вершинам:

$$p\left(x_A(t) = V_i\right) = \frac{1}{n}, \text{ где } V_i \in V_n. \quad (7)$$

Подставляем (7) в (6). Тогда вероятность захвата вершины V_i за время T равна:

$$P_c(T) = 1 - \left(1 - \frac{1}{n}\right)^T.$$

Найдем вероятность необнаружения маршрута за один шаг j=1. В момент времени t, если:

- защитник D с маршрутом k_i в случайной вершине $V_i \in V$;
- атакующий занимают случайную вершину-объект V_i, через которую проходит один из k_i маршрутов D.

Тогда вероятность, что атакующий A не попал на маршрут защитника в этот момент:

$$P_{\text{нет захвата маршрута за шаг j=1}} = 1 - \frac{n_{v_i}}{\sum_{k=1}^{n}\left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}\right)}, \quad (8)$$

то есть атакующий на шаге j=1 в одной из вершин; с вероятностью p, что она совпадет с любой из случайных в сформированных маршрутах

$$p = \frac{n_{v_i}}{\sum_{k=1}^{n}\left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}\right)}.$$

Вероятность непопадания на объект – вершину, включенную в маршрут, за j шагов определяется при независимом движении A и D на каждом шаге:

$$P_{\text{нет захвата маршрута за j шаг}} = \left(1 - \frac{n_{v_i}}{\sum_{k=1}^{n}\left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}\right)}\right)^{j}. \quad (9)$$

Вероятность попадания на объект – вершину, включенную в маршрут, за j шагов – это противоположное событие. Тогда:

$$P(j) = 1 - \left(1 - \frac{n_{v_i}}{\sum_{k=1}^{n}\left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_I}\right)}\right)^{j}. \quad (10)$$

Интерпретация уравнения (10):

- при j=0 : $P(j$=0)=0;
- при $j \to \infty$: $P(j) \to 1$ (атакующий обнаружит действующий маршрут);
- при большом количестве маршрутов k_i вероятность захвата любого маршрута атакующим A растет быстрее.

На рис. 2 показано как вероятность захвата (время захвата T=j) маршрута защитника $P(j)$ возрастает с увеличением числа шагов j для различных соотношений k_i/n – числа маршрутов k_i и числа вершин n ПС сети:

- чем больше k_i маршрутов прокладывается по сети, тем быстрее происходит захват;
- при меньшем n (граф меньшего размера) вероятность захвата выше при тех же k_i.

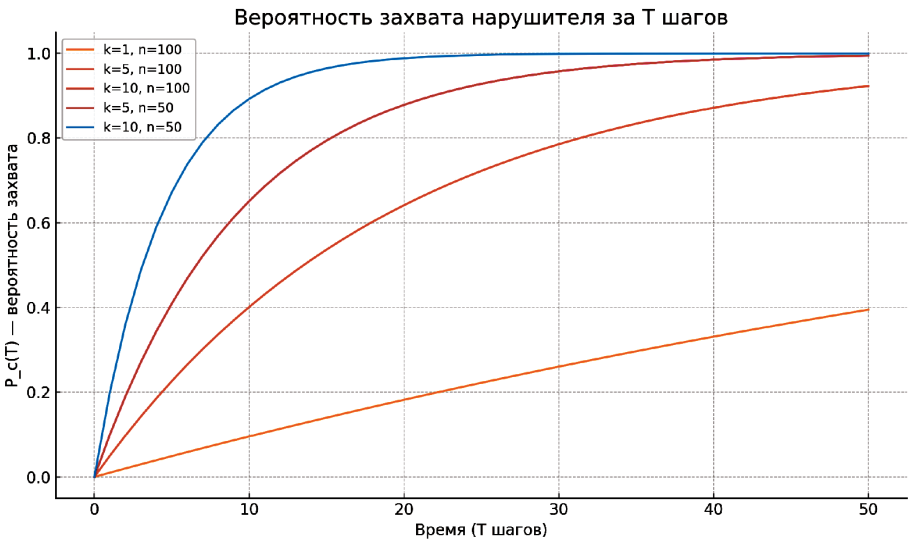

Рис. 2. Вероятность захвата маршрута защитника за j шагов, j=T

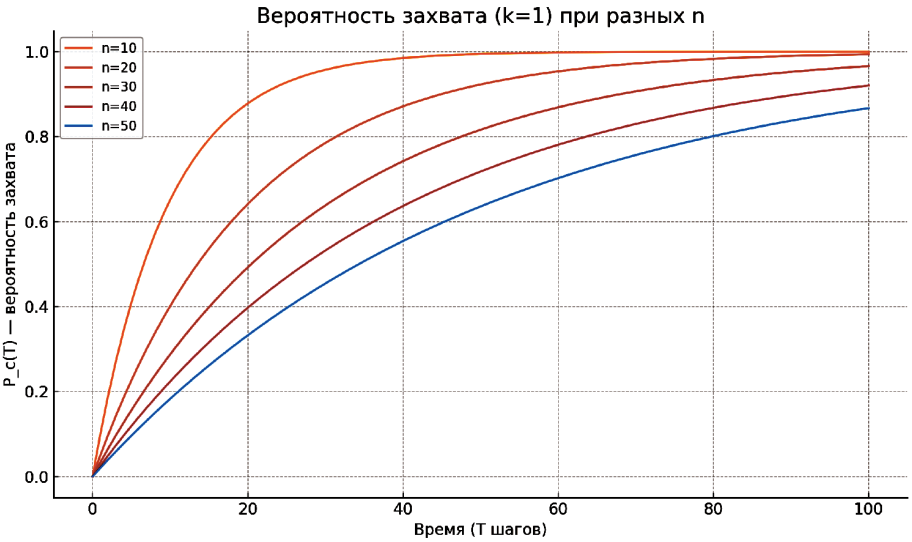

Рис. 3 Вероятность захвата маршрута при одном атакующем и одном маршруте (k = 1) и различных размерах графа n = 10, 20, 30, 40, 50

На рис. 3 показаны зависимости вероятности захвата маршрута при одном атакующем и одном маршруте для различных размеров графа. Из рис. 3 следует:

- чем меньше граф (n), тем быстрее вероятность захвата растет;
- при n = 10 захват вероятен уже за ~20 шагов;
- при n = 50 требуется гораздо больше шагов, чтобы достичь высокой вероятности (например, 80–90%).

На рис. 4 показано, как увеличение числа маршрутов k_i при фиксированном числе вершин n=30 влияет на скорость захвата:

- при k_i=1 вероятность растет медленно, нужно ~30–40 шагов для высокой вероятности;
- при k=5 уже за ~15 шагов вероятность захвата достигает ~80%;
- при k=10 вероятность захвата достигает 90% примерно за 10 шагов;
- при k=20 захват почти гарантирован за первые 5–6 шагов.

Таким образом, на основании полученных данных можно сделать следующий вывод: увеличение числа вершин n ядра ПС сети при постоянно заданном

количестве маршрутов k снижает вероятность захвата вершины в сформированных маршрутах.

Рассмотрим решение задачи определения времени захвата атакующим *A* вершины V_i за j шагов, по которой передается информационный поток, за время его существования t_{M_k}.

Решение. Оценку времени захвата атакующим вершины случайного маршрута проведем с использованием геометрического распределения [16]. Условия, применения геометрического распределения:

- каждый шаг j – независим;
- защитник и атакующий независимо и случайно выбирают вершины на каждом шаге;
- вероятность захвата постоянна на каждом шаге;
- на каждом шаге вероятность того, что защитник и атакующий окажутся в одной вершине, определяется из (8) и равно

$$p = \frac{n_{v_i}}{\sum_{k=1}^{n}\left(\bigcup_{i=1}^{n_1} M_{k_i}^{RUE_l}\right)}.$$

Геометрическое распределение описывает число шагов до первого успеха в последовательности независимых испытаний, где в каждом испытании вероятность успеха равна p. Формула геометрического распределения:

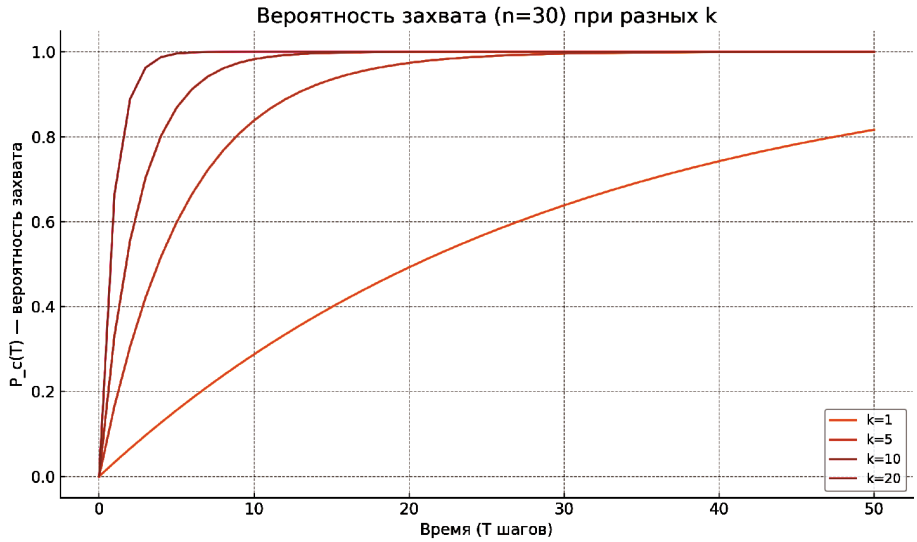

Рис. 4 Вероятность захвата при k_i и постоянном числе вершин

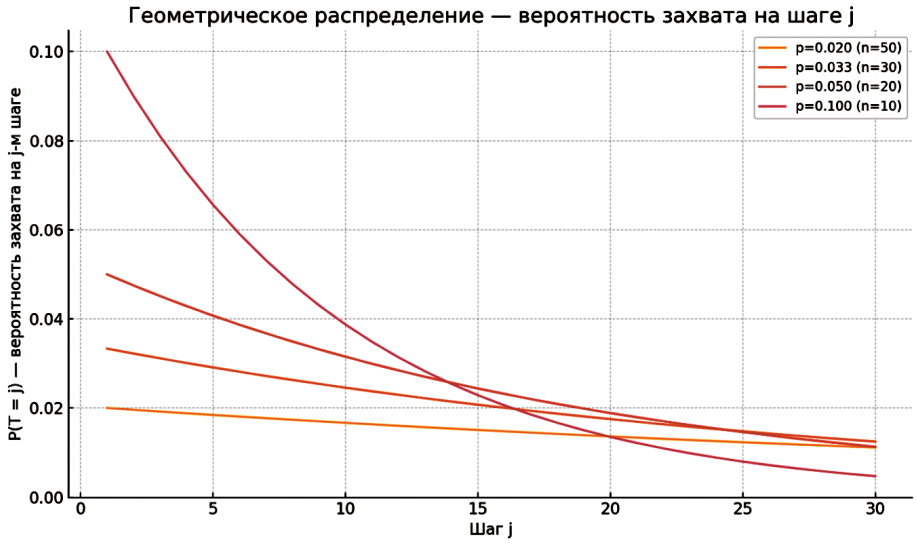

Рис. 5 Вероятность захвата вершины от времени t=J

$$\mathbb{P}[J = t] = (1-p)^{t-1} \cdot p, \qquad (11)$$

где J – количество шагов до первого успеха;

p – вероятность успеха на каждом шаге в момент времени t–1;

$(1–p)^{t-1}$ – ни одного успеха в первых t–1 шагах;

p – и успех на t-м шаге.

Захват возможен только в одном месте. Если в текущем шаге не произошло захвата, идем к следующему шагу, и процесс повторяется с той же вероятностью. Поскольку каждый шаг – одно испытание, захват – это успех и каждое испытание независимо, то мы имеем классическую ситуацию геометрического распределения времени до первого успеха. Распределение времени (10) захвата за j шагов:

$$\mathrm{Geom}(p) -> P[J \le j] = (1-p)^{j-1} \cdot p. \qquad (12)$$

Ожидаемое (среднее) время захвата: $\mathbb{P}[J] = \frac{1}{p} = \frac{n}{k_i}$.

На рис. 5 приведены значения времени t=j геометрического распределения Geom(p) с осью шагов j. Он показывает, как меняется вероятность захвата на каждом шаге при разных значениях p=k_i/n. J определяет время проходящее от начала процесса захвата до его завершения. Длительность существования информационного потока определяется объемом передаваемой информации и обычно составляет t_{M_k}=3–5 с. Время захвата вершины – объекта атакующим лежит в пределах 15–20 с. Исходя из этого, можно сделать вывод, что для осуществления перехвата трафика атакующий должен завладеть как можно большим количеством вершин-объектов, через которые передаются информационные потоки.

Заключение

Рассмотрена модель построения системы защиты информации, реализующей принцип «защитника от атакующего». Получена оценка вероятности захвата атакующим вершины графа, через которую проходит маршрут.

Предложено, при реализации многоуровневой системы защиты для предотвращения перехвата информационных потоков использовать динамически организуемые доверенные маршруты в условиях полносвязности.

Предложенная методика позволяет оценить уменьшение вероятности захвата вершин полносвязной сети. Предложенная методика позволяет оценить вероятность захвата вершин полносвязной сети в зависимости от длительности передаваемого сообщения.

Благодарность. Работа выполнена за счет бюджетного финансирования в рамках государственного задания от 20.03.2025 № 103-00001-25-02.

Список литературы

1. Попов П.А., Розенберг Е.Н., Сабанов А.Г. и др. Комплексная безопасность АСУ ТП объектов КИИ железнодорожного транспорта // Надежность. 2024. Том: 24 №: 4. С. 48-57. DOI: 10.21683/1729-2646-2024-24-4-48-57

2. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. Утв. приказом ФСТЭК России от 02.06.2020 г. № 76.

3. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утв. приказом ФСТЭК России от 25.12.2017 г. № 239.

4. Сайт Oxidized: Система управления конфигурациями сетевого оборудования // Oxidized [электронный ресурс]. URL: https://bubnovd.net/post/blogger/система-управления-конфигурациями-oxidized/ (дата обращения: 14.04.2025).

5. Дмитриева Ю.С. Сравнительный анализ методов управления сетевыми ресурсами в сетях SDN // Труды учебных заведений связи. 2022. № 8. С. 73-83.

6. Волков А.С., Баскаков А.Е. Разработка алгоритма многопутевой маршрутизации в программно-конфигурируемых сетях связи // T-Comm – Телекоммуникации и Транспорт. 2021. № 5. С. 17-23.

7. Черников А.С., Паус А.С. Многопоточная маршрутизация в программно-конфигурируемых сетях // Радиооптика. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 06. С. 35-46. DOI: 10.7463/rdopt.0616.0850725

8. Eiman Alotaibi. A tutorial on software-defined networks emulation // Journal of Engineering Research. DOI:10.1016/j.jer.2023.12.005

9. Mohammad Nowsin Amin Sheikh, I-Shyan Hwang, Muhammad Saibtain Raza. A Qualitative and Comparative Performance Assessment of Logically Centralized SDN Controllers via Mininet Emulator // Computers. 2024. Vol. 13(4). P. 85. DOI: 10.3390/computers13040085

10. Программно-определяемые сети SDN // Cloud Networks [электронный реурс]. URL: https://cloudnetworks.ru/inf-tehnologii/programmno-opredelyaemye-seti-sdn/ (дата обращения: 14.04.2025).

11. Mudassar Hussain Nadir Shah, Rashid Amin. Software-Defined Networking: Categories, Analysis, and Future Directions // Sensors. 2022. Vol. 22(15). P. 5551. DOI: 10.3390/s22155551

12. Ivakhnenko A.G. Longterm forecasting and management of complex systems. Kiev: Technics, 1975. 310 p.

13. Алексеев В.М., Чичков С.Н. Защита информации в интеллектуальных транспортных системах управления городским транспортом // Надежность. 2022. Том 22. № 3. С. 62-68.

14. Вахний Т.В., Tyu A.K. Матрично-игровая программа с выбором критерия для определения оптимального набора средств защиты компьютерной системы // Математические структуры и моделирование. 2016. № 2(38). С. 103-115.

15. Савченко С.О., Капчук Н.В. Алгоритм построения модели нарушителя в системе информационной безопасности с применением теории игр // Динамика систем, механизмов и машин. 2017. Том 5. № 4. DOI: 10.25206/2310-9793-2017-5-4-84-90

16. Колчин В.Ф. Геометрическое распределение. В кн.: Большая российская энциклопедия : [в 35 т.] / гл. ред. Ю. С. Осипов. М.: Большая российская энциклопедия, 2004-2017.

References

1. Popov P.A., Rozenberg E.N., Sabanov A.G., Shubinsky I.B. Integrated Safety of ACS of Railway CII Facilities. *Dependability* 2024;24(4):48-57. (in Russ.) DOI: 10.21683/1729-2646-2024-24-4-48-57

2. [Information security requirements that define the levels of trust to the information security and information technology protection tools. Approved by the order of the FSTEC of Russia dated 06.02.2020 No. 76]. (in Russ.)

3. [Safety requirements for significant facilities of critical information infrastructure of the Russian Federation. Approved by the order of the FSTEC of Russia dated 12.25.2017 No. 239]. (in Russ.)

4. [Oxidized: Network equipment configuration management system]. (accessed 14.04.2025). Available at: https://bubnovd.net/post/blogger/система-управления-конфигурациями-oxidized/

5. Dmitrieva J. Comparative Analysis of Network Resource Management Methods in SDN. *Proc. Of Telecom. Universities* 2022;8(1):73-83. (in Russ.)

6. Volkov A.S., Baskakov A.E. Development of a multipath routing algorithm in software-defined communication networks. *T-Comm* 2021;15(9):17-23. (in Russ.)

7. Chernikov A.S., Paus A.S. Multi-threaded Routing in Software-defined Networking. *Radiooptics of the Bauman MSTU* 2016;6:35-46. DOI: 10.7463/rdopt.0616.0850725

8. Alotaibi E. A tutorial on software-defined networks emulation. *Journal of Engineering Research*. DOI:10.1016/j.jer.2023.12.005

9. Mohammad Nowsin Amin Sheikh, I-Shyan Hwang, Muhammad Saibtain Raza. A Qualitative and Comparative Performance Assessment of Logically Centralized SDN Controllers via Mininet Emulator. *Computers* 2024;13(4):85. DOI: 10.3390/computers13040085

10. Cloud Networks. (accessed 14.04.2025). Available at: https://cloudnetworks.ru/inf-tehnologii/programmno-opredelyaemye-seti-sdn/

11. Mudassar Hussain Nadir Shah, Rashid Amin. Software-Defined Networking: Categories, Analysis, and Future Directions. *Sensors* 2022;22(15):5551. DOI: 10.3390/s22155551

12. Ivakhnenko A.G. Longterm forecasting and management of complex systems. Kiev: Technics; 1975. (in Russ.)

13. Alekseev V.M., Chichkov S.N. Information security in intelligent mass transit management systems. *Dependability* 2022;22(3):62-68. (in Russ.)

14. Vahniy T.V., Guts A.K., Novikov N.Y. Matrix-game program with selection criterion for determination of optimal tool set for computer system protection. *Mathematical Structures and Modeling* 2016:2(38):103-115. (in Russ.)

15. Savchenko S.O., Kapchuk N.V. Algorithm of creation of model of the violator in the information security system with application of game theory. *Dynamics of Systems Mechanisms and Machines* 2017;5(4):84-89. (in Russ.) DOI:10.25206/2310-9793-2017-5-4-84-89

16. Kolchin V.F. Geometric distribution. In: Osipov Yu.S., chief editor. The Great Russian Encyclopaedia: [in 35 volumes]. Moscow: The Great Russian Encyclopaedia; 2004-2017. (in Russ.)

Сведения об авторах

Алексеев Виктор Михайлович – доктор технических наук, профессор, профессор кафедры «Управление и защита информации», Российский университет транспорта (МИИТ), Москва, Российская Федерация, e-mail: alekseevvm@rambler.ru.

Баранов Леонид Аврамович – доктор технических наук, профессор, заведующий кафедрой «Управление и защита информации», Российский университет транспорта (МИИТ), Москва, Российская Федерация.

Чичков Сергей Николаевич – аспирант кафедры «Управление и защита информации», старший преподаватель кафедры «Высшая математика», Российский университет транспорта (МИИТ), Москва, Российская Федерация, e-mail: seriozha.tchichkov@yandex.ru.

About the authors

Victor V. Alekseev, Doctor of Engineering, Professor, Professor of the Department of Management and Protection of Information, Russian University of Transport (MIIT), Moscow, Russian Federation, e-mail: alekseevvm@rambler.ru.

Leonid A. Baranov, Doctor of Engineering, Professor, Head of the Department of Management and Protection of Information, Russian University of Transport (MIIT), Moscow, Russian Federation.

Sergey N. Chichkov, post-graduate student, Department of Management and Protection of Information, Senior Teacher, Department of Higher Mathematics, Russian University of Transport (MIIT), Moscow, Russian Federation, e-mail: seriozha.tchichkov@yandex.ru.

Вклад авторов в статью

Алексеев В.М. Разработка и оценка моделей.

Баранов Л.А. Разработка и оценка моделей.

Чичков С.Н. Выполнение расчетов, оформление результатов.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.