УДК 007

ОЦЕНКА ХАРАКТЕРИСТИК КИБЕРПРОСТРАНСТВА НА ОСНОВЕ РЕЗУЛЬТАТОВ ТЕСТИРОВАНИЯ СЕТЕЙ ИЗ ЕГО СОСТАВА

***Закалкин П.В.*[1]**

Ключевые слова: *разведка в киберпространстве, вероятность, услуга связи, доступность, уравнение регрессии.*

Цель исследования: *определение вероятностных характеристик киберпространства, а в частности вероятности построения составного канала между двумя произвольными точками киберпространства с целью проведения дальнейших исследований киберпространства.*

Методы исследования: *системный анализ, сравнительный анализ, методы теории вероятности.*

Полученные результаты: *на основе открытых исходных данных, представленных общественными организациями, рассчитана вероятность построения составного канала между двумя произвольными точками киберпространства; выведено уравнение регрессии для дальнейших расчетов.*

Научная новизна: *предложен подход к определению вероятностных характеристик киберпространства, а в частности произведен расчет вероятности построения составного канала между двумя произвольными точками киберпространства.*

Введение

Киберпространство сформировалось в результате развития систем связи и их трансформации в информационно-коммуникационные системы с последующей интеграцией с навигационными, технологическими, экономическими и другими процессами в различных областях деятельности человечества. Произошла интеграция процессов генерации, сбора, передачи, обработки и распределения информационных ресурсов в автоматизированном и автоматическом режиме, что непрерывно порождает множество новых технологических процессов в различных областях деятельности человечества, в том числе в управлении отдельными индивидуумами, группами и обществом в целом [1,2].

Киберпространство в корне изменило подход к предоставлению услуг связи, который фактически не изменялся с 1990-х гг. Для корпоративных систем управления (КСУ) появление киберпространства означало поэтапный отказ от использования в системах связи собственных линейных средств в пользу ресурсов и услуг, предоставляемых киберпространством [3,4]. Современные КСУ, используя оконечное оборудование,

[1] Закалкин Павел Владимирович, кандидат технических наук, сотрудник, Академия Федеральной Службы Охраны Российской Федерации, Орёл, Россия. E-mail: pzakalkin@mail.ru, https://orcid.org/0000-0003-2946-2586

подключаются к киберпространству (посредством заключения договора с оператором связи) и осуществляют информационный обмен между своими элементами.

Киберпространство предоставляет свои ресурсы и информационные услуги любому потребителю, имеющему техническую возможность подключения к нему, что приводит к функционированию различных систем управления (в том числе антагонистических) в едином пространстве на единых ресурсах. Это позволяет вести разведывательную деятельность в киберпространстве.

Поиск и сбор данных в информационных ресурсах киберпространства осуществляется средствами технической компьютерной разведки (ТКР), предназначенными для ведения разведки по открытым источникам и осуществления несанкционированного доступа. Большая часть трафика из Европы в Азию, Океанию, Африку и Южной Америку передается через магистральные линии, проходящие непосредственно через США или соединенные с линиями США, и контролируются ими[2]. Используя центры контроля трафика, весь передаваемый трафик проходит через центры обработки глобальной системы сбора и обработки разведывательной информации (например «Эшелон»[3]). Все перехватываемые данные подвергаются автоматизированной контекстной обработке в целях выявления наиболее важных сообщений, классификации по различным признакам и распределения по базам.

Соответственно, элементы КСУ подключаясь к киберпространству непроизвольно накладывают на себя следующие основные ограничения:

- становятся объектом разведки иностранных спецслужб;
- обеспечение связи между элементами КСУ (фактически возможности построения составного канала от одного элемента до другого) целиком зависит от киберпространства;
- трафик, циркулирующий между элементами КСУ проходит по маршрутам, строящимся операторами связи, и в том числе выходит за пределы РФ.

Киберпространство является сложным, динамически изменяющимся, малоизученным пространством. Данное исследование в первую очередь направлено на оценку вероятностных характеристик киберпространства, а в частности затрагивает вероятность построения составного канала от одного элемента киберпространства до

---

[2] Континентальные сети интернета [Электронный ресурс] URL:https://gea.site/2018/04/638/?ysclid=lzmq3bhcgh658438344

[3] 1) Осторожно, Вас слышит «Эшелон»! (экскурс в историю и настоящее англоговорящей системы глобального электронного шпионажа) [Электронный ресурс] URL: https://habr.com/ru/articles/64386/

2) Глобальная система радиоэлектронной разведки ECHELON, что она представляет и насколько опасна [Электронный ресурс] URL: https://overclockers.ru/blog/Pitfalls/show/83169/globalnaya-sistema-radioelektronnoj-razvedki-echelon-chto-ona-predstavlyaet-i-naskolko-opasna

другого с учетом необходимости предоставления услуг с приемлемым качеством. Исследование основывается на открытых данных, предоставляемых общественными организациями, декларирующими в качестве своей основной цели тестирование сетей, входящих в киберпространство.

В рамках статьи под киберпространством будем понимать искусственное неоднородное технологическое пространство с множеством разноуровневых органов оперативного и технологического управления, процесс создания и эксплуатации которого не предопределяется требованиями одной системы управления, а функционирует в интересах множества разнородных, в том числе антагонистических систем управления. При этом свойства киберпространства зависят как от характеристик собственных элементов, так и от объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей [5,6].

Средства применяемые для разведки в киберпространстве

Построение телекоммуникационной составляющей киберпространства на основе зарубежного телекоммуникационного оборудования с использованием иностранного программного обеспечения и протоколов привело к тому, что ТКР беспрепятственно размещает в киберпространстве средства разведки, информационно-технических воздействий и программные закладки. В таблице 1 представлены примеры средств компьютерной разведки, данные о которых имеются в открытых источниках (в том числе и были обнародованы Эдвардом Сноуденом).

Таблица 1.

Средства компьютерной разведки

Название	**Кем используется**	**Возможности**
Stellar Wind	АНБ США	Слежение и поиск сообщений электронной почты, телефонных разговоров, финансовых операций и интернет-активность в целом
PRISM	АНБ США	Просмотр электронной почты, фотографий, видео, прослушивание голосовых и видеочатов, отслеживание пересылаемых файлов
CO-TRAVELER	АНБ США	Отслеживание передвижения владельцев сотовых телефонов и выявление сети их контактов
Dropmire	АНБ США	Аппаратные и программные закладки, внедряемые в телекоммуникационные системы
X-Keyscore	АНБ США, Управление радиотехнической обороны Австралии и др.	Более чем 700 серверов, расположенных в США и на территории стран - союзников США

Название	Кем используется	Возможности
Tempora	Центр правительственной связи Великобритании, АНБ США	Сбор данных из перехватов телефонных разговоров и интернет-трафика
Karma Police	Центр правительственной связи Великобритании	Сбор метаданных в сети Интернет
MAINWAY	АНБ	База данных АНБ, содержащая метаданные звонках, совершенных через крупнейшие телефонные компании США
NarusInsight	ФБР	Прослушивание и анализ данных сетевого трафика в сети Интернет

В качестве примеров технических средств разведки можно указать средства, представленные в каталоге ANT. Каталог ANT – документ АНБ США содержащий перечень устройств и технологий электронного шпионажа, находящихся в распоряжении ANT (подразделение АНБ). Каталог представлен в открытом доступе, также часть средств более подробно рассмотрена в ряде публикаций[4].

Разведка киберпространства ведется не только напрямую подчиненными иностранным киберкомандованиям подразделениями, но и другими организациями, в том числе общественными, так или иначе связанными с различными структурами иностранных государств. Примерами таких структур могут служить RIPE, GlobalCheck, M-Lab и др[5].

На организации RIPE остановимся более подробно поскольку она является типовой, и предоставляемые ей данные в дальнейшем будут использоваться для расчетов в проводимом исследовании.

Организацией RIPE создан проект Atlas, целью которого является повышение устойчивости функционирования сети Интернет. Сутью проекта является тестирование сети добровольно установленными на своем сетевом оборудовании датчиками. Этим достигается не только заявленная проектом цель, но и фактически обеспечивается возможность ведения ТКР и реализации деструктивных программных воздействий (ДПВ).

К 2024 году установлено более 12,5 тыс. датчиков, которые суммарно единовременно производят более 20 тыс. измерений различных параметров

[4] 1) Клянчин А.И. Каталог закладок АНБ (SPIGEL). Часть 1. Инфраструктура // Вопросы кибербезопасности №2(3) 2014 С. 60–65.
2) Клянчин А.И. Каталог закладок АНБ (SPIGEL). Часть 2. Рабочее место оператора // Вопросы кибербезопасности №4(7) 2014 С. 60–68.

[5] 1) Официальный портал RIPE [Электронный ресурс] URL: RIPE (дата обращения 05.06.2024)
2) Официальный портал GlobalCheck [Электронный ресурс] URL: GlobalCheck (дата обращения 05.06.2024)
3) Официальный портал M-Lab [Электронный ресурс] URL: M-Lab (дата обращения 05.06.2024)

киберпространства и получают более 7,5 тыс. результатов в секунду. Распределение датчиков на территории мира представлено на рисунке 1.

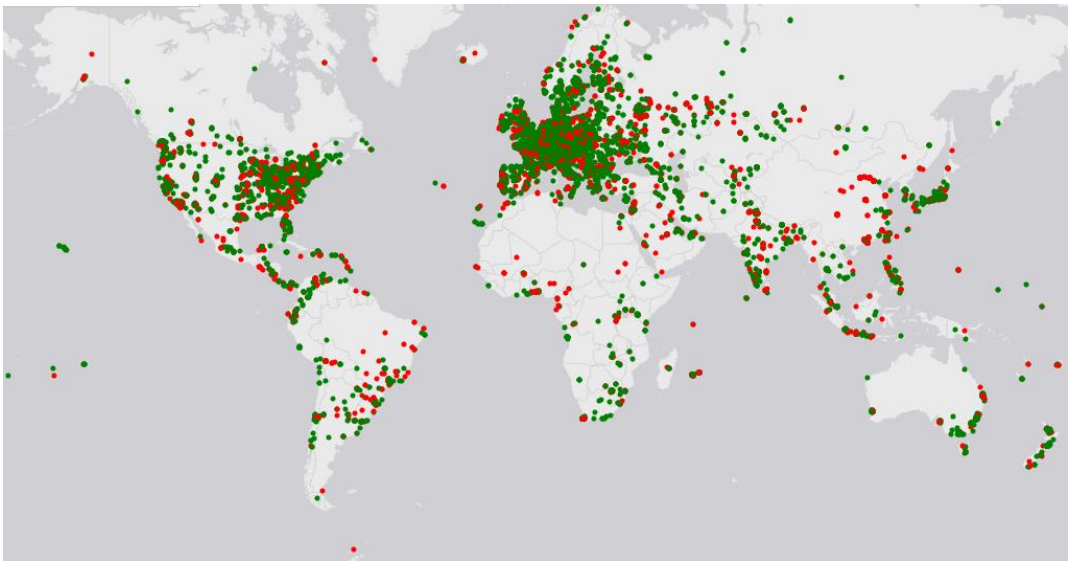

Рис. 1. Датчики Atlas на карте мира

По состоянию на 2024 год на территории РФ функционирует 734 датчика (включая отключенные в момент проверки). Распределение датчиков на территории РФ представлено на Рис. 2.

Датчик представляет собой сетевое устройство, не имеющее интерфейса для непосредственного взаимодействия с пользователем, взаимодействие осуществляется через управляющий сервер Atlas.

Система состоит из т.н. «якорей» и «зондов», которые рассылаются бесплатно в ответ на поданную заявку. Сервис устроен следующим образом: «зонды» получают и выполняют задания по произведению тех или иных измерений, а «якоря» сами имеют разные сетевые сервисы, в отношении которых можно проводить подобные измерения.

Рис. 2. Датчики Atlas на территории России

Кроме этого, «зонды» получают задания на проверку связности (доступности) или скорости связи с теми или иными адресами. Пользователи RIPE Atlas также могут выполнять индивидуальные измерения, чтобы получить данные о собственных сетях. Вся информация, собранная «якорями» и «зондами», агрегируется и обрабатывается на центральных серверах Ripe Atlas.

Проекты M-Lab и GlobalCheck во многом похожи на RIPE Atlas и также посредством бесплатной раздачи и установки датчиков в различных частях киберпространства собирают информацию о различных параметрах функционирования киберпространства с последующим агрегированием этой информации и ее изучением. Совокупная информации собираемая этими структурами, позволяет получать целостную картину состояния киберпространства фактически в режиме реального времени.

Анализируя места расположения датчиков на территории РФ, можно сделать вывод, что в подавляющем большинстве они расположены рядом с высшими военными учебными заведениями, воинскими частями, объектами, имеющими стратегическое значение (заводы, аэропорты, крупные центры связи). При этом количество датчиков увеличивается, если в населенном пункте имеется точка обмена трафиком.

Обобщая вышесказанное, можно сделать вывод, что основной функцией данного типа устройств является сбор разведывательных данных о параметрах киберпространства, потребителях и других процессах, протекающих в нем.

Формулирование гипотез

В общем случае большинство систем мониторинга (в том числе проектов M-Lab и GlobalCheck) включают в себя три основных элемента [7-10]:

- датчики, собирающие информацию о контролируемом объекте;
- подсистема обработки получаемой информации;
- система принятия решения, осуществляющая управляющие воздействия в отношении контролируемого объекта, либо в отношении датчиков, если необходимо осуществление дополнительных, нестандартных и т. п. измерений.

Функционирование такой системы требует постоянной (либо максимально приближенной к этому) связи (с заданным качеством) между элементами, осуществляющими мониторинг и подсистемой сбора и обработки получаемой информации. Другими словами, должно существовать некое множество маршрутов, позволяющее построить составной канал от элементов, осуществляющих мониторинг к подсистеме сбора и обработки получаемой информации. При этом, построенный канал должен обеспечивать

качество, приемлемое для обмена информацией между датчиками и подсистемой сбора и обработки получаемой информации.

Основываясь на принципах работы (из открытых источников) и карты размещения датчиков RIPE Atlas можно выдвинуть следующие гипотезы:

1) все точки киберпространства взаимоувязаны, и в любой произвольный момент времени возможно построить составной канал из одной произвольной точки киберпространства в другую;

2) построение составного канала из одной произвольной точки киберпространства в другую осуществляется с качеством, приемлемым для предоставления информационной услуги.

Учитывая, что структура физических сетей, являющихся основой киберпространства, их связанность, потоки передачи данных, логическая структура и т.д. имеется в виде разрозненных данных у множества операторов связи (с соответствующими пометками отнесения их к конфиденциальной информации, коммерческой тайне и т.п.), составить глобальную физическую структуру киберпространства фактически не представляется возможным. В связи с этим, предлагается использовать данные из открытых источников (в частности, RIPE Atlas) для расчета вероятности построения составного канала из одной произвольной точки киберпространства к другой.

Порядок осуществления расчетов

Основная суть измерений датчиками RIPE Atlas заключается в выполнении утилиты ping из произвольной точки киберпространства (один из датчиков) к другим датчикам, расположенным по всему миру. Утилита ping отправляет ряд пакетов от узла источника к узлу получателю и ждет ответа от него, отображая время, через которое получен ответ. В нашем случае получение ответа от узла получателя говорит о том, что посредством киберпространства до него возможно построить составной канал.

Из всего массива предоставляемых RIPE Atlas данных произвольно выбраны 4 точки (датчика), для каждой из точек произвольно выбрано 5 дат (начиная с 2020 г. и заканчивая мартом 2024 г.). Результаты измерений занесены в таблицы 2–5.

Представленные в таблицах 2–5 данные являются усредненными значениями измерений за два часа. Согласно открытых данных обращение к каждому из датчиков Ripe Atlas осуществляется в среднем раз в 10 мин. (время округлено в большую сторону), соответственно за два часа для каждого из датчиков проводится 12 измерений: $2 \cdot 60 мин \diagup 10 мин = 12$.

Всего за выбранные даты проводилось 203016 измерений, учитывая, что для каждого датчика за 2 часа осуществляется 12 измерений, то общее количество измерений для 4-х точек и 5 дат будет составлять: $203016 \cdot 12 = 2436192$. Соответственно, представленные в таблицах 2–5 данные основаны на 2,44 млн. измерений. Такое количество измерений позволяет нам говорить о вероятностных характеристиках доступа к случайным точкам в киберпространстве.

При расчете вероятности построения составного канала из одной произвольной точки киберпространства к другой будем исходить из наихудшего случая и считаем все датчики, о которых нет информации – недоступными. Зная общее количество датчиков и их распределение по времени ping, возможно рассчитать вероятность построения составного канала из точки киберпространства (относительно которой проводились измерения) к случайному датчику (а фактически к случайной точке киберпространства). Эта вероятность рассчитана и представлена в каждой таблице в графе «вероятность».

В таблицах 2 – 5 представлены полученные данные.

Таблица 2.

Измерения для точки 1

Дата	< 10 ms	< 20 ms	< 30 ms	< 40 ms	< 50 ms	< 100 ms	< 200 ms	< 300 ms	> 300 ms	НИ	НД	Всего датчиков
10.09.20	3008	1993	921	375	218	478	247	74	41	1431	83	8869
20.01.21	3589	2289	936	430	246	362	109	35	24	1312	72	9404
08.09.22	4224	2520	844	350	207	401	219	55	23	1312	79	10234
11.01.23	4606	2729	896	379	205	430	232	48	28	973	108	10634
06.03.24	5694	3189	1006	483	241	512	292	47	23	85	41	11613
Вероятность	0,416	0,251	0,091	0,040	0,022	0,043	0,022	0,005	0,003	0,108		

Поле «НИ» – нет информации о датчике, поле «НД» – нет доступа к датчику, поле «Всего датчиков» – общее количество датчиков на заданную дату.

Таблица 3.

Измерения для точки 2

Дата	< 10 ms	< 20 ms	< 30 ms	< 40 ms	< 50 ms	< 100 ms	< 200 ms	< 300 ms	> 300 ms	НИ	НД	Всего датчиков
10.09.20	3144	1888	873	386	210	497	241	92	27	1430	81	8869
20.01.21	3571	2231	1064	414	222	334	131	32	13	1313	79	9404
08.09.22	4316	2586	867	348	202	325	138	39	21	1314	78	10234

11.01.23	4765	2845	894	359	207	323	141	31	12	973	84	10634
06.03.24	5939	3283	1062	434	222	345	175	20	20	72	41	11613
Вероятность	0,428	0,253	0,094	0,038	0,021	0,036	0,016	0,004	0,002	0,108		

Таблица 4.

Измерения для точки 3

Дата	< 10 ms	< 20 ms	< 30 ms	< 40 ms	< 50 ms	< 100 ms	< 200 ms	< 300 ms	> 300 ms	НИ	НД	Всего датчиков
10.09.20	2284	1616	1125	532	311	789	525	124	25	1431	107	8869
20.01.21	2541	1984	1345	660	461	625	277	77	16	1312	106	9404
08.09.22	2718	2047	1341	703	487	891	527	80	12	1312	116	10234
11.01.23	2728	2124	1593	819	507	919	722	103	15	973	131	10634
06.03.24	2939	2705	1906	1185	614	827	437	138	22	754	86	11613
Вероятность	0,260	0,206	0,144	0,077	0,047	0,080	0,049	0,010	0,002	0,125		

Таблица 5.

Измерения для точки 4

Дата	< 10 ms	< 20 ms	< 30 ms	< 40 ms	< 50 ms	< 100 ms	< 200 ms	< 300 ms	> 300 ms	НИ	НД	Всего датчиков
10.09.20	1538	1570	1221	791	511	991	490	167	45	1430	115	8869
20.01.21	1672	1670	1380	877	630	1046	516	130	52	1311	120	9404
08.09.22	1894	1858	1408	867	761	1255	493	235	48	1313	102	10234
11.01.23	2132	1998	1560	949	892	1265	562	203	20	976	77	10634
06.03.24	2480	2258	1631	1224	1055	1373	736	182	26	626	22	11613
Вероятность	0,191	0,184	0,142	0,093	0,076	0,117	0,055	0,018	0,004	0,120		

Исходя из данных, представленных в таблицах 2–5 был произведен расчет вероятности построения составного канала из произвольной точки киберпространства к произвольному датчику (а фактически к произвольной точке киберпространства). Полученные в таблице 6 значения вероятностей отражают вероятность построения составного канала к произвольной точке киберпространства с значением ping, не превышающим указанное.

Таблица 6.

Обобщенные значения вероятности доступа для киберпространства

Значение ping	< 10 ms	< 20 ms	< 30 ms	< 40 ms	< 50 ms	< 100 ms	< 200 ms	< 300 ms	> 300 ms	НД и НИ
Вероятность	0,324	0,224	0,118	0,062	0,041	0,07	0,035	0,009	0,002	0,115

Согласно открытых источников[6] приемлемым значением ping являются значения до 100 ms, значения до 200 ms являются приемлемыми для обращения к сайтам, базам данных и т.д., но медиасервисы будут работать медленнее. Значения ping более 200 ms говорит о проблемах на маршруте передачи данных до узла получателя. Исходя из этого, приемлемыми значениями будет считать значения ping, не превышающие 200 ms. Соответственно, исходя из рассчитанных и представленных в таблице 6 значений вероятности для каждого времени ping, можно рассчитать вероятность построения составного канала к случайному узлу киберпространства с ping, не превышающим 200 ms. Расчеты показывают, что с вероятностью 0,874 можно построить составной канал к произвольному узлу киберпространства с ping, не превышающим 200 ms:

$$P_{\text{дост}} = 0{,}874 \quad \text{при ping} < 200 \text{ ms}.$$

Таким образом, в настоящее время существующие характеристики киберпространства по своим параметрам позволяют построить составной канал с приемлемым качеством из произвольной точки киберпространства к любому узлу киберпространства с вероятностью 87%.

Учитывая тот факт, что при расчете вероятности доступа из одного узла киберпространства к любому случайному узлу в киберпространстве исходим из наихудшего случая (т.е. все узлы к которым нет доступа и узлы, о которых нет информации, считаем недоступными), то вероятность отказа в построении составного канала из произвольной точки киберпространства к любому произвольному узлу киберпространства составит 11 %.

Здесь необходимо оговориться, что сама по себе физическая связанность с произвольной точкой киберпространства будет (проводные, беспроводные и др. линии связи). Однако, на логическом уровне доступ будет заблокирован по какой-либо причине. Например, из-за санкций в отношении РФ, заблокирован доступ к ряду ресурсов, с одной стороны странами, которые ввели санкции, а с другой стороны нашей страной в отношении недружественных стран. Конечно, существует множество способов обхода этих блокировок, однако для этого необходимо применять специализированные средства. В

[6] 1) Что такое пинг и как его понизить? [Электронный ресурс] URL: https://dominternet.ru/blog/chto-takoe-ping-kakoy-dolzhen-byt-ping-v-skorosti-interneta/

2) Как снизить пинг и оптимизировать скорость онлайн-игр [Электронный ресурс] URL: https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-improve-game-performance

нашем же исследовании мы рассматриваем наихудший случай в условиях отсутствия этих средств.

С учетом этого, и того, что вероятность построения составного канала рассчитывалась с учетом ограничений, округления значений в меньшую сторону, отнесения узлов о которых нет информации к разряду узлов, к которым нет доступа, то реальное значение вероятности построения составного канала на практике может быть значительно выше.

Далее необходимо установить характер зависимости между полученными значениями вероятности. Для чего на первоначальном этапе построим диаграммы, отображающие распределения вероятности построения составного канала к произвольному узлу киберпространства и выбранных точек (рисунок 3 - 7).

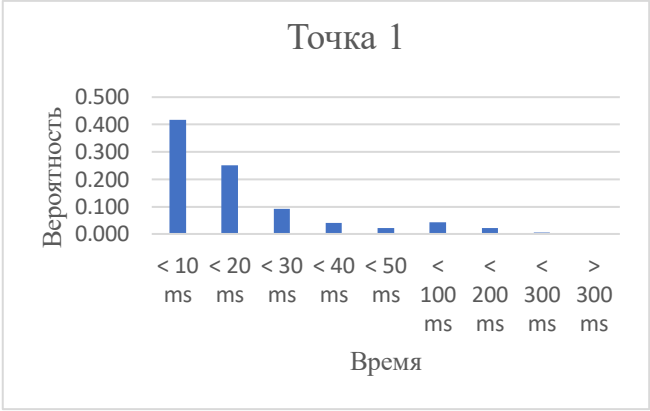

Рис. 3. Графическое отображение распределения вероятности построения составного канала к произвольному узлу киберпространства из точки 1

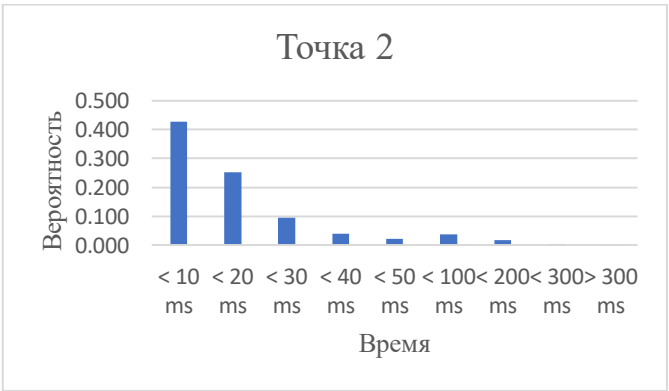

Рис. 4. Графическое отображение распределения вероятности построения составного канала к произвольному узлу киберпространства из точки 2

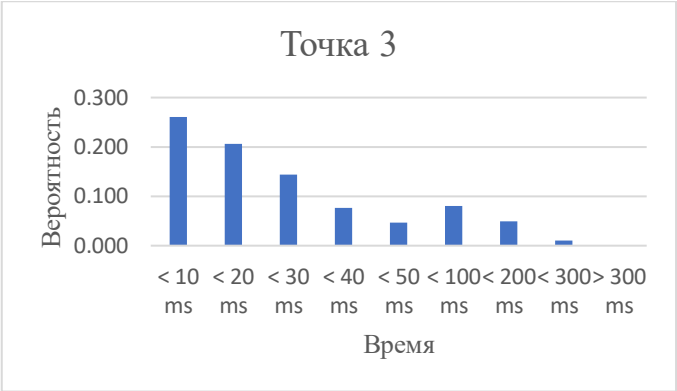

Рис. 5. Графическое отображение распределения вероятности построения составного канала к произвольному узлу киберпространства из точки 3

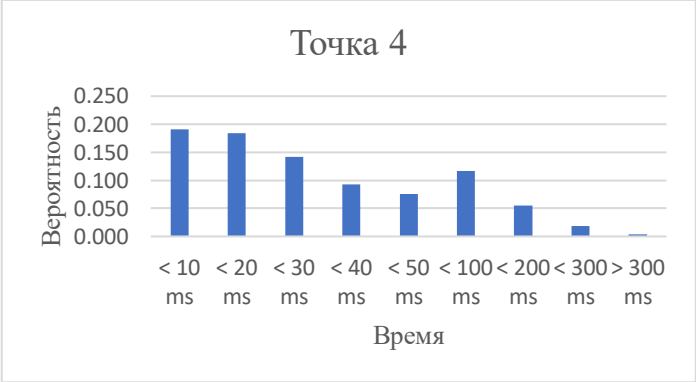

Рис. 6. Графическое отображение распределения вероятности построения составного канала к произвольному узлу киберпространства из точки 4

На рисунке 7 построено распределение вероятности построения составного канала к произвольному узлу из произвольной точки киберпространства

Рис. 7. Графическое отображение распределения вероятности построения составного канала к произвольному узлу произвольной точки киберпространства

На рисунках 3–7 четко прослеживается экспоненциальная регрессия, характеризующаяся резким спадом значения вероятности в начале и его последующим замедлением в дальнейшем и приближением к нулю. Некоторое возрастание значений

вероятности на 100 ms и 200 ms прежде всего вызвано изменением масштаба шкалы измерения (переход с десятков ms на сотни ms).

Уравнение экспоненциальной регрессии имеет вид – $\hat{y} = e^{a+bx}$ (1)

Коэффициенты a и b, описывающие взаимосвязь между X и Y, рассчитывались по формулам: $b = \frac{n\sum x_i \ln y_i - \sum x_i \cdot \sum \ln y_i}{n\sum x_i^2 - (\sum x_i)^2}$ и $a = \frac{1}{n}\ln y_i - \frac{b}{n}\sum x_i$. (2)

Коэффициент корреляции рассчитывался как: $R = \sqrt{1 - \frac{\sum (y_i - \hat{y}_i)^2}{\sum (y_i - \bar{y})^2}}$, (3)

где $\bar{y} = \frac{1}{n}\sum y_i$

Коэффициент детерминации рассчитывался как: R^2

Средняя ошибка аппроксимации рассчитывалась как:

$$\bar{A} = \frac{1}{n}\sum \left| \frac{y_i - \hat{y}_i}{y_i} \right| \cdot 100\% \quad (4)$$

Рассчитанные значения квадратичной, показательной и экспоненциальной регрессии приведены в таблице 7.

Таблица 7.

Значения квадратичной, показательной и экспоненциальной регрессии

	Квадратичная регрессия	Показательная	Экспоненциальная
Коэффициент корреляции	0.75	0.73	0.73
Коэффициент детерминации	0.57	0.54	0.54
Средняя ошибка аппроксимации (%)	190	43	43

Ошибка аппроксимации в первую очередь вызвана тем, что используемые значения начинаются не от нуля и не однороден масштаб шкалы измерения (по X).

В результате расчетов получено следующее графическое отображение экспоненциальной регрессии (Рис. 8).

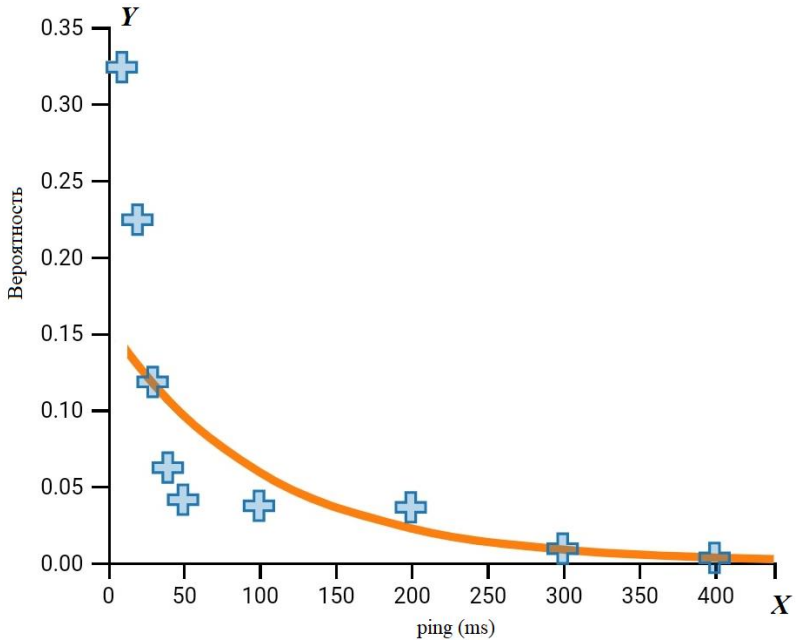

Рис. 8. Графическое отображение экспоненциальной регрессии

Выведено следующее уравнение регрессии, позволяющее прогнозировать значение *y* при заданном значении *x*:

$$y = e^{-1.7685-0.0099x}. \qquad (5)$$

На первоначальном этапе, пока информация, предоставляемая датчиками RIPE Atlas, находится в открытом доступе, для расчетов возможно ее использование. Необходимо понимать, что это временная мера, т.к. RIPE Atlas может свернуть программу, закрыть доступ к информации для посторонних пользователей, предоставлять недостоверную информацию и т.д., что приведет к невозможность проведения расчета.

В текущий момент времени для расчетов возможно использовать полученное уравнение регрессии, которое будет верно до принципиального изменения структуры киберпространства. Однако, в дальнейшем необходима собственная система мониторинга в киберпространстве, позволяющая получать в режиме реального времени собственные значения, необходимые для расчета вероятности доступа.

Выводы

В статье предложен подход к определению вероятностных характеристик киберпространства, а в частности произведен расчет вероятности построения составного канала между двумя произвольными точками киберпространства.

Рассчитанные значения вероятностей позволят:

- проводить дальнейшие исследования киберпространства: осуществлять анализ свойств киберпространства для формирования требований к элементам и разработки

алгоритмов их функционирования; формировать данные для оптимизации процессов управления ресурсами киберпространством; и т.д.;

- служить исходными данными для исследований в области информационной безопасности;
- строить аналитико-имитационные модели киберпространства.

Достоверность исследования подтверждается:

- использованием апробированных исходных данных, характеризующих параметры киберпространства;
- использованием ключевых положений теории вероятности.

Литература

1. Иванов С.А. Устойчивость сетей связи общего пользования в условиях глобализации // Известия Тульского государственного университета. Технические науки. 2021. № 9. С. 86–90.
2. Коцыняк М.А., Лаута О.С., Нечепуренко А.П. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного противоборства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 1-2 (127-128). С. 58–62.
3. Закалкин П.В. Аспекты использования киберпространства в интересах корпоративных систем управления // Труды Научно-исследовательского института радио. 2021. № 4. С. 23–32.
4. Иванов С.А., Стародубцев Ю.И. Теорема о представлении непрерывного многопараметрического сигнала с ненулевой дисперсией дискретными отсчетами // Системы управления, связи и безопасности. 2021. № 2. С. 12–36
5. Закалкин П.В. Аспекты использования киберпространства в интересах корпоративных систем управления // Труды Научно-исследовательского института радио. 2021. № 4. С. 23–32.
6. Стародубцев Ю.И., Закалкин П.В. Структурно-функциональный анализ конфликтной ситуации между государственной системой обеспечения информационной безопасности и иностранной системой деструктивных воздействий // Вопросы кибербезопасности. 2024. № 4 (62). С. 82–91.
7. Белов А.С., Добрышин М.М. Предложение по удаленному мониторингу программных средств автономных комплексов связи // Авиакосмическое приборостроение. 2021. № 6. С. 13–20.
8. Гречишников Е.В., Зубачев А.Б., Сазыкин А.М., Добрышин М.М., Берлизев А.В. Предложения по повышению быстродействия распределенной системы мониторинга компьютерных сетей, интегрированных в единую сеть электросвязи // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2017. № 3-4 (105-106). С. 24–29.
9. Нижегородов А.В., Закалкин П.В., Стародубцев П.Ю., Кабанов А.С. Роль мониторинга в системе обнаружения, предупреждения и ликвидации последствий компьютерных атак // Промышленные АСУ и контроллеры. 2013. № 7. С. 67–71.
10. *Закалкин П.В., Стародубцев Ю.И.*, Майбурд С. В. Предложения по паспортизации российского сегмента киберпространства // В сборнике: Современное состояние и перспективы развития инфокоммуникационных сетей связи специального назначения. Материалы научно-практической конференции. Санкт-Петербург, 2024. С. 79–84

ASSESSMENT OF THE CHARACTERISTICS OF CYBERSPACE BASED ON THE RESULTS OF TESTING NETWORKS FROM ITS COMPOSITION

Zakalkin P.V.[7]

Keywords: *intelligence in cyberspace, probability, communication service, availability, regression equation.*

The purpose of the study*: is to determine the probabilistic characteristics of cyberspace, and in particular the probability of building a composite channel between two arbitrary points of cyberspace in order to conduct further research on cyberspace.*

The results obtained: *based on open source data provided by public organizations, the probability of building a composite channel between two arbitrary points in cyberspace is calculated; a regression equation is derived for further calculations.*

Scientific novelty: *an approach to determining the probabilistic characteristics of cyberspace is proposed, and in particular, the probability of constructing a composite channel between two arbitrary points of cyberspace is calculated.*

Research methods: *system analysis, comparative analysis, methods of probability theory.*

References

1. Ivanov S.A. Ustojchivost' setej svjazi obshhego pol'zovanija v uslovijah globalizacii // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. 2021. № 9. S. 86–90.
2. Kocynjak M.A., Lauta O.S., Nechepurenko A.P. Metodika ocenki ustojchivosti informacionno-telekommunikacionnoj seti v uslovijah informacionnogo protivoborstva // Voprosy oboronnoj tehniki. Serija 16: Tehnicheskie sredstva protivodejstvija terrorizmu. 2019. № 1-2 (127-128). S. 58–62.
3. Zakalkin P.V. Aspekty ispol'zovanija kiberprostranstva v interesah korporativnyh sistem upravlenija // Trudy Nauchno-issledovatel'skogo instituta radio. 2021. № 4. S. 23–32.
4. Ivanov S.A., Starodubcev Ju.I. Teorema o predstavlenii nepreryvnogo mnogoparametricheskogo signala s nenulevoj dispersiej diskretnymi otschetami // Sistemy upravlenija, svjazi i bezopasnosti. 2021. № 2. S. 12–36
5. Zakalkin P.V. Aspekty ispol'zovanija kiberprostranstva v interesah korporativnyh sistem upravlenija // Trudy Nauchno-issledovatel'skogo instituta radio. 2021. № 4. S. 23–32.
6. Starodubcev Ju.I., Zakalkin P.V. Strukturno-funkcional'nyj analiz konfliktnoj situacii mezhdu gosudarstvennoj sistemoj obespechenija informacionnoj bezopasnosti i inostrannoj sistemoj destruktivnyh vozdejstvij // Voprosy kiberbezopasnosti. 2024. № 4 (62). S. 82–91.
7. Belov A.S., Dobryshin M.M. Predlozhenie po udalennomu monitoringu programmnyh sredstv avtonomnyh kompleksov svjazi // Aviakosmicheskoe priborostroenie. 2021. № 6. S. 13–20.
8. Grechishnikov E.V., Zubachev A.B., Sazykin A.M., Dobryshin M.M., Berlizev A.V. Predlozhenija po povysheniju bystrodejstvija raspredelennoj sistemy monitoringa komp'juternyh setej, integrirovannyh v edinuju set' jelektrosvjazi // Voprosy oboronnoj tehniki. Serija 16: Tehnicheskie sredstva protivodejstvija terrorizmu. 2017. № 3-4 (105-106). S. 24–29.
9. Nizhegorodov A.V., Zakalkin P.V., Starodubcev P.Ju., Kabanov A.S. Rol' monitoringa v sisteme obnaruzhenija, preduprezhdenija i likvidacii posledstvij komp'juternyh atak // Promyshlennye ASU i kontrollery. 2013. № 7. S. 67–71.
10. Zakalkin P.V., Starodubcev Ju.I., Majburd S. V. Predlozhenija po pasportizacii rossijskogo segmenta kiberprostranstva // V sbornike: Sovremennoe sostojanie i perspektivy razvitija infokommunikacionnyh setej svjazi special'nogo naznachenija. Materialy nauchno-prakticheskoj konferencii. Sankt-Peterburg, 2024. S. 79–84

[7] Pavel V. Zakalkin, Ph.D., employee, Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: pzakalkin@mail.ru, https://orcid.org/0000-0003-2946-2586