чими процессами укладчика для повышения эффективности регулирования ровности асфальтобетонного покрытия с улучшенными показателями качества процесса управления на основе учета динамики гидравлических элементов.

Библиографические ссылки

1. Денисенко В. В. ПИД-регуляторы: принципы построения и модификации // Соврем. технологии автоматизации. 2006. № 4–5. С. 66–74.

2. Костельов М. П., Пахаренко Д. В., Бринкс З. К. Как правильно выбрать и настроить асфальтоукладчик [Электронный ресурс] // Дорожная техника – 2007 : кат.-справ. 2007. URL: http://www.mrmz.ru/article/v70/article1.htm (дата обращения: 7.04.2012).

3. Интеллектуальные системы автоматического управления / под ред. И. М. Макарова, В. М. Лохина. М. : Физматлит, 2001.

4. Иванчура В. И., Прокопьев А. П. Оптимизация следящей системы автоматического управления // Вестник СибГАУ. 2011. Вып. 5 (38). С. 44–49.

V. I. Ivanchura, A. P. Prokopiev, R. T. Emelianov

MODEL OF A TRACKING SYSTEM OF AUTOMATIC CONTROL WITH FUZZY SLIDER

This paper is devoted to theoretical and application problems of tracking systems of automatic control. A model of such tracking system of automatic control with fuzzy slider is designed, with the help of the MATLAB&Simulink program. The results of simulation studies are presented

Keywords: asphalter, working body of compacting, asphalt – concrete mix, automatic control, tracking systems, fuzzy logic.

УДК 004.738

С. В. Исаев

АНАЛИЗ ДИНАМИКИ ИНТЕРНЕТ-УГРОЗ СЕТИ КРАСНОЯРСКОГО НАУЧНОГО ЦЕНТРА СИБИРСКОГО ОТДЕЛЕНИЯ РОССИЙСКОЙ АКАДЕМИИ НАУК*

Выполнен анализ интернет-угроз на основе многолетних данных работы сети Красноярского научного центра Сибирского отделения Российской академии наук. Выявлены основные тенденции развития опасных факторов и структура источников опасностей.

Ключевые слова: Интернет, вирусы, электронная почта, защита информации.

В связи с развитием информационных и телекоммуникационных технологий, а также с расширением круга пользователей, подключенных к сети Интернет, задачи обеспечения информационной безопасности становятся все более актуальными. В Институте вычислительного моделирования Сибирского отделения (СО) Российской академии наук (РАН) на протяжении пяти последних лет ведется работа по сбору данных о возможных информационных угрозах, таких как попытки вторжений, вирусная активность и несанкционированные почтовые рассылки. Целью данной работы является попытка анализа полученных данных и их сравнение с общемировыми тенденциями.

Проблемы защиты информации широко обсуждаются в интернет-среде [1] и печатных источниках. При этом предлагаются не только методы и решения для частных случаев, но и общие принципы разработки систем защиты [2; 3]. Однако для комплексной защиты сети в каждом конкретном случае требуется вырабатывать адекватное решение, учитывающее особенности организации сети, виды защищаемой информации, круг пользователей и основанное на анализе динамики интернет-угроз.

Корпоративная сеть Красноярского научного центра (КНЦ) объединяет девять организаций Сибирского отделения РАН и соединена как с сетью Интернет, так и с сетью образовательных учреждений Красноярска. Общая длина линий магистральных линий связи – более 15 км, число пользователей во всех организациях – более 1 000. Большинство узлов сети не содержат какой-либо конфиденциальной информации и нуждаются в защите только от вредоносных воздействий.

Трехуровневая архитектура корпоративной сети (рис. 1) позволяет максимально эффективно управлять информационными потоками и их защитой. Критически важные узлы отделены от подсети общего информационного потока средствами сетевой адресации и межсетевыми экранами. Конфигурация внутренней сети скрыта от внешнего мира при помощи механизма преобразования адресов и использования в качестве посредника прокси-сервера. Имеются средства регистрации пользователей, обеспечивающие однозначную классификацию трафика и протоколирование в системном журнале.

*Работа выполнена при финансовой поддержке гранта ФЦП «Научные и научно-педагогические кадры инновационной России на 2009–2013 гг.» (ГК № 02.740.11.0621 от 29.03.2010).

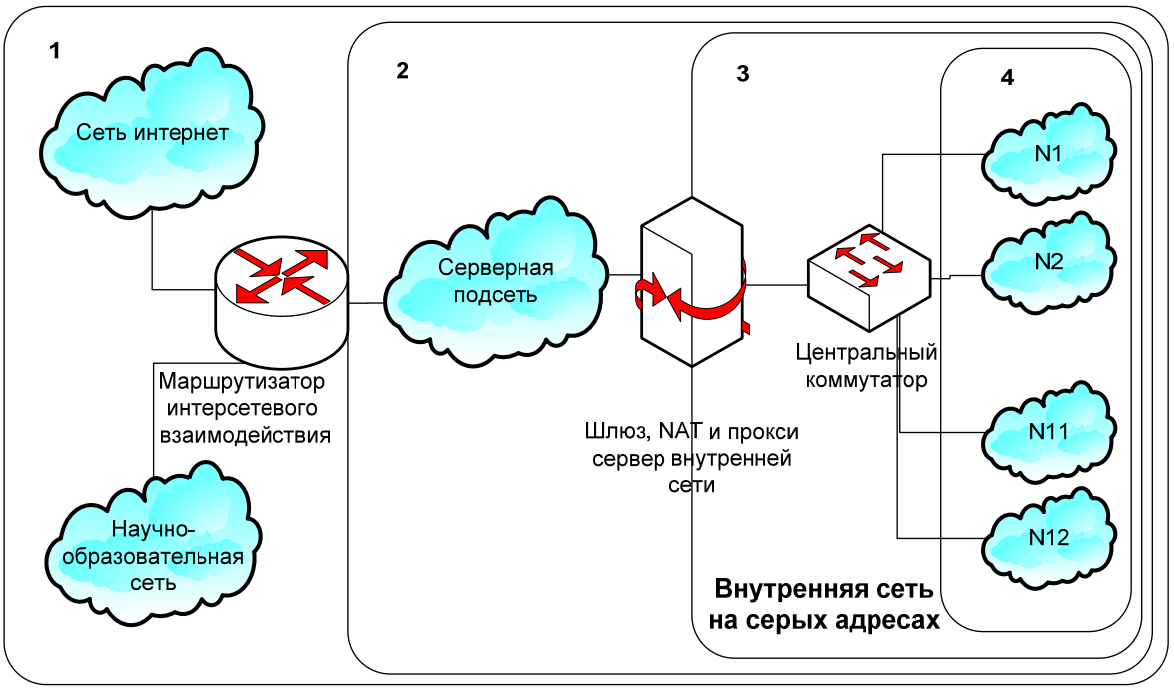

Рис. 1. Структура корпоративной сети

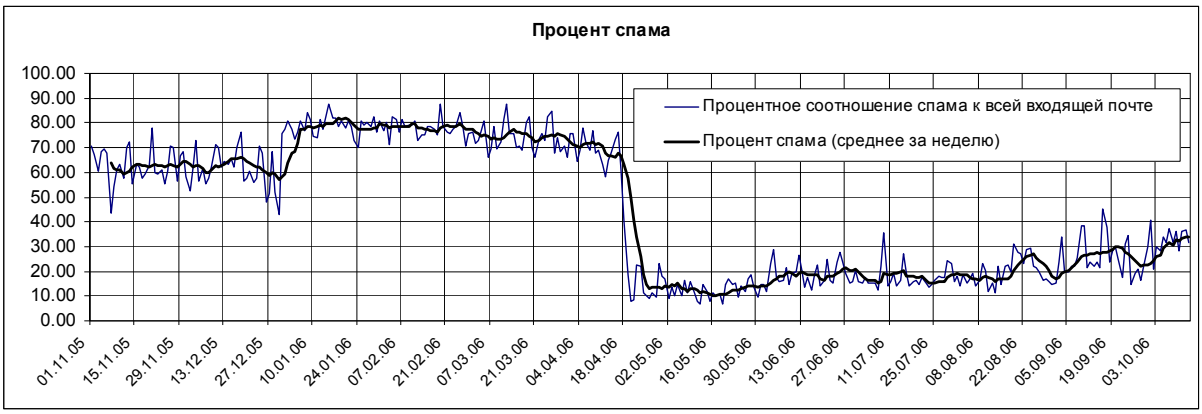

Рис. 2. Изменение процента спама в 2006 г. после введения «серых» списков

Для анализа тенденций безопасности были взяты три источника:

– журнал системы обнаружения вторжений, функционирующий на маршрутизаторе интерсетевого взаимодействия и шлюзе корпоративной сети;

– журнал антивирусной системы корпоративного почтового сервера КНЦ СО РАН;

– журнал системы пометки спама корпоративного почтового сервера КНЦ СО РАН.

Начало наблюдений относится к 2006 г., когда спам составлял от 80 до 30 %, среднее ежедневное количество писем с вирусами – 50, в отдельные периоды – более 200. После введения «серых» списков на сервер электронной почты количество спама уменьшилось в 4 раза (рис. 2). Но, к сожалению, далее этот метод перестал работать столь эффективно.

В 2007 г. процент спама стабилизировался на уровне 50 %, среднее количество вирусов составляло около 50 с подъемом в периоды эпидемии до 400 (рис. 3). В этой связи можно отметить, что на протяжении нескольких лет (2006–2008 гг.) вирусные эпидемии фиксировались в новогодние праздники и в конце лета.

Для 2008 г. были характерны следующие показатели:

– средний процент спама – около 70 %, причем количество российских источников спама превысило количество источников спама из США;

– среднее количество вирусов в почте – около 10, в периоды эпидемий – более 100;

– количество срабатываний системы обнаружения попыток вторжений составило 4 226, распределение по странам см. на рис. 5.

Кроме того, в 2008 г. было закрыто большое количество ботнет-сетей, что привело к резкому снижению процента спама в почте к концу года до 30 %. На протяжении 2009 г. этот показатель сохранялся примерно на том же уровне, что и вирусная активность.

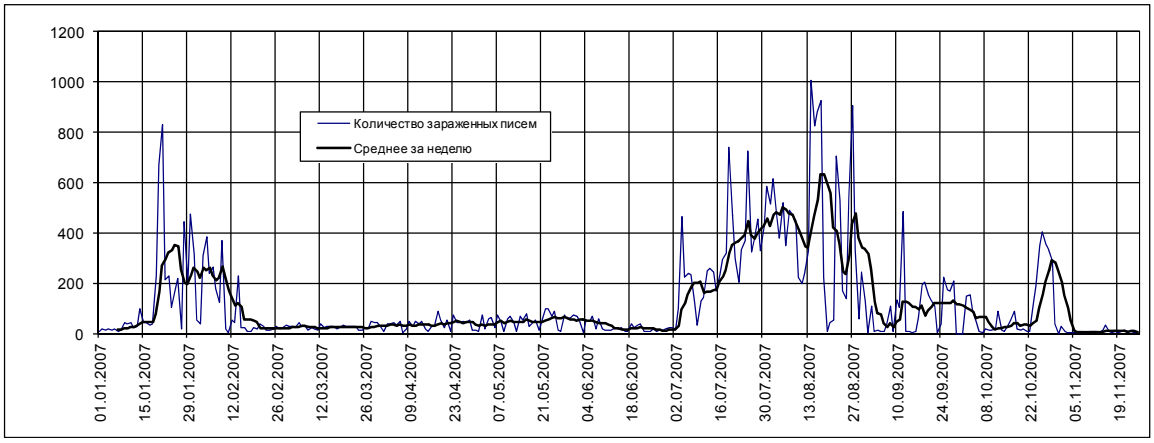

Рис. 3. Вирусные эпидемии в 2007 г.

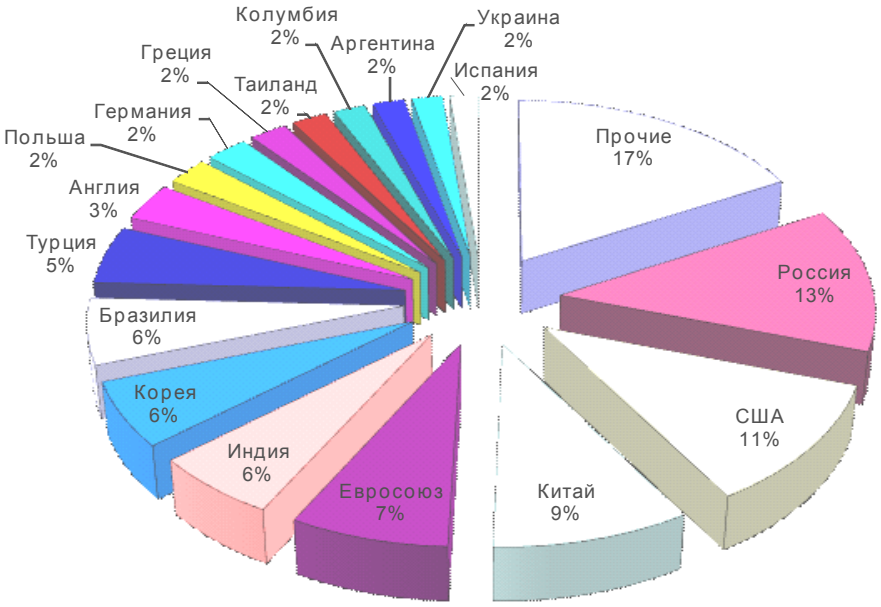

Рис. 4. Источники спама за 2008 г.

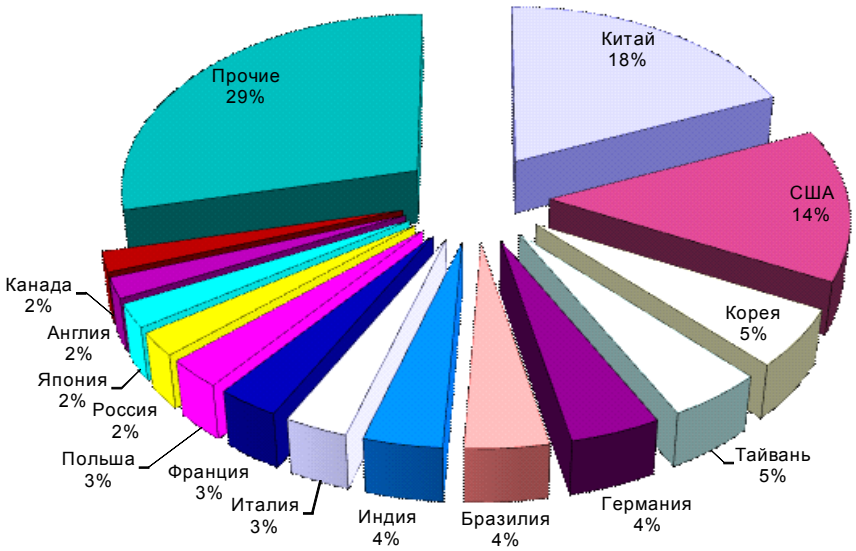

Рис. 5. Источники попыток несанкционированного входа в 2008 г.

В 2010 г. процент спама в почте снизился до 20 %, среднее количество вирусов не превысило 10, периоды массовых вирусных эпидемий отсутствовали. Доля российских источников спама превысила долю США в 2 раза и составила 11 % (рис. 6).

В 2011 г. количество обнаруженных вирусов в почте достигло 3 500. Среди лидеров по источникам спама появились азиатские страны: Индия, Корея, Вьетнам. Китай же, наоборот, переместился в нижнюю часть рейтинга.

Количество срабатываний системы обнаружения попыток вторжений в 2011 г. превысило 70 000, среди лидеров – Китай, США, Канада, Индия, Япония и страны Евросоюза (рис. 7), причем источники попыток несанкционированного доступа не связаны с вирусами.

По результатам пятилетних наблюдений была составлена сводная таблица (см. с. 24), содержащая распределение источников интернет-угроз по наиболее активным странам.

Построенные на основе этих данных графики наглядно иллюстрирует динамику по рассылке спама (рис. 8) и источникам вирусов (рис. 9) в крупнейших странах.

Рис. 6. Источники спама за 2010 г.

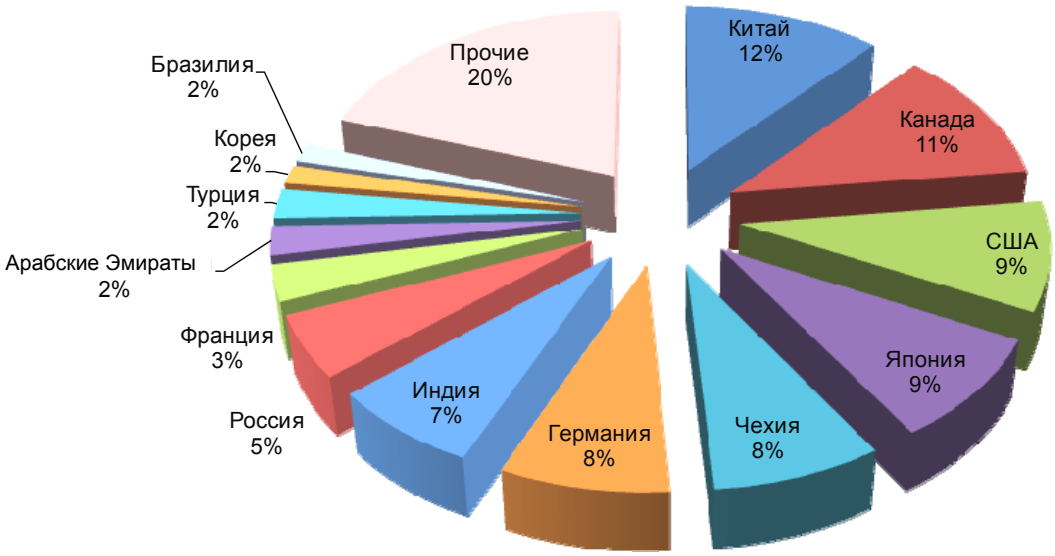

Рис. 7. Источники попыток несанкционированного доступа за 2011 г.

Основные источники интернет-угроз за 2007–2011 гг.

Страна	Спам, %				Вирусы, %			Сканирования, %			Сумма
	2007	2008	2010	2011	2008	2010	2011	2007	2008	2011	2011
США	25	11	6	6	37	9,4	17	12,9	14	9	32
Россия	6	13	11	11	17	14	15	2	2	5	31
Индия	3	6	5	5	4	3,9	7	4,2	4	7	19
Китай	4	9	3	3	1	2,7	2	17,5	18	12	17
Германия	4	3	3	3	2	2,2	2	4,8	4	8	13
Бразилия	2	6	5	5	1	4,8	2	3,9	4	2	9
Корея	8	6	5	5	3	5,1	2	6,4	5	2	9
Франция	4	3	3	3	2	1,5	1	4,4	3	3	7
Польша	2	2	3	3	1	1	2	3,2	3	0,5	5
Англия	3	3	2	2	2	3,1	2	2	2	1	5

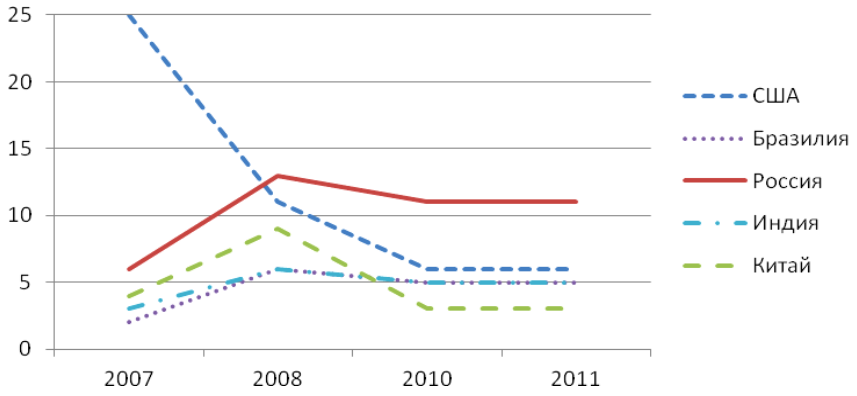

Рис. 8. Динамика рассылки спама по отдельным странам

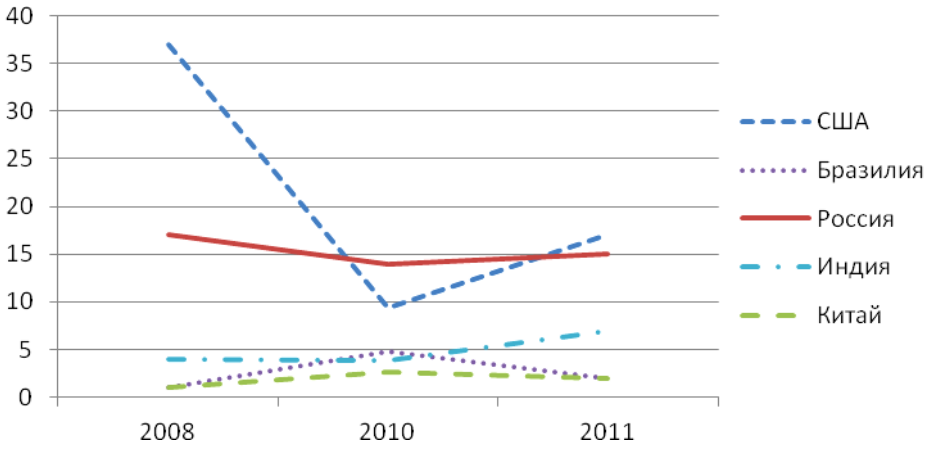

Рис. 9. Динамика источников вирусов по странам

Анализ полученной информации позволяет выявить следующие тенденции:

– активное внедрение компьютерных технологий и Интернета в страны азиатского и латиноамериканского регионов (Индия, Китай, Корея, Бразилия) и связанный с этим всплеск вирусной и спам-активности;

– общее снижение вирусной и спам-активности более чем в 5 раз, очевидно за счет развития средств защиты;

– увеличение попыток вторжений более чем в 15 раз;

– успешную борьбу со спамом в США и Китае.

Несмотря на то что собранные данные относятся к сетям с научной спецификой, отмеченные закономерности в целом согласуются с общемировыми [1]. В частности, подтверждается тезис о насыщении азиатских стран компьютерными технологиями и выравнивании вирусной и спам-активности. К сожалению, в России пока не наблюдается тенденции к уменьшению источников опасностей и по динамике развития Россия похожа на Индию и Бразилию. Внедрение новых, оснащенных встроенной защитой операционных систем и сетевых клиентов позволяет сдерживать распространение интернет-угроз. Однако сеть Интернет по-прежнему остается небезопасной, так как происходит постоянное обнаружение новых уязвимостей сетевых сервисов, и при несвоевременном их устранении вероятность несанкционированного вторжения резко увеличивается.

Библиографические ссылки

1. Гудкова Д. Планета, захваченная спамерами // SECURELIST.RU : ежедн. интернет-изд. 2011. 20 сент. URL: http://www.securelist.com/ru/analysis/208050717/Planeta_zakhvachennaya_spamerami (дата обращения: 20.10.2011).

2. Соколов А. В., Шаньгин В. Ф. Защита информации в распределенных корпоративных сетях и системах. М. : ДМК Пресс, 2002.

3. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети – анализ технологий и синтез решений. М. : ДМК Пресс, 2004.

S. V. Isaev

ANALYSIS OF INTERNET THREATS DYNAMICS OF THE NETWORK OF KRASNOYARSK SCIENTIFIC CENTER SB RAS

The work is devoted to the analysis of Internet threats, made on the basis of long-term data of the network of Krasnoyarsk scientific center of the Siberian Branch of Russian Academy of Science. The main tendencies of development of dangerous factors and the structure of danger sources are determined.

Keywords: Internet, viruses, e-mail, data security.

УДК 538.915

А. А. Кузубов, Ю. Г. Михалев, М. В. Сержантова

ВЛИЯНИЕ ВАКАНСИЙ НА МАГНИТНОЕ УПОРЯДОЧЕНИЕ В МОНОСЛОЕ h-BN

Исследовано влияние вакансий бора и азота, а также расстояния между ними на магнитное упорядочение в структуре монослоя гексагонального нитрида бора.

Ключевые слова: монослой гексагонального нитрида бора, теория функционала плотности, электронная структура, вакансии.

Одним из важных вопросов физики конденсированного состояния остается установление взаимосвязи между наличием в системе электронов проводимости и магнитными свойствами материала [1; 2]. Факт появления магнитного упорядочения в плоских структурах типа графена и гексагонального нитрида бора (h-BN) оценивался ранее как маловероятный, поскольку в атомах углерода, бора и азота отсутствуют *d*- и *f*-электроны. Тем не менее данный эффект объясняется кристаллическими [3–7] и структурными дефектами [8].

В работах [9; 10] показано, что точечные дефекты (вакансии) в графене обладают локальными магнитными моментами, взаимодействие которых с электронами проводимости приводит к появлению в системе эффекта Кондо [2; 11–13]. В работе [9] авторы предполагают, что с помощью модификаций решетки графена вакансиями могут быть реализованы магнитноупорядоченные системы на основе углеродных наноструктур, в которых возможны переходы «ферромагнетик–антиферромагнетик» [14].

Монослой h-BN с вакансиями – это еще один пример появления намагниченности в плоских структурах [15–17], когда спонтанная намагниченность в отсутствии дефектов не возникает. В работе [15] была получена спонтанная намагниченность в присутствии примесей замещения (C_B, C_N) или вакансий (V_B, V_N) в структуре h-BN. Спин-поляризованные расчеты для C_B- и C_N-дефектов показывают намагниченность монослоя h-BN, которая составляет 1,0 μ_B на один дефект. При вакансионных дефектах V_B и V_N в системе наблюдается спиновая поляризация, которая приводит к появлению магнитных моментов с величинами 3,0 и 1,0 μ_B соответственно. Это объясняется тем, что при удалении атома азота из монослоя h-BN структура имеет только один неспаренный электрон, а при