УДК 004.02

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКОГО ПРОГРАММИРОВАНИЯ В РЕШЕНИИ ЗАДАЧИ ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Картак В.М., Башмаков Н.М.
Уфимский государственный авиационный технический университет, Уфа, РФ
E-mail: KVmail@mail.ru, nail.bashmakov@gmail.com

Целью исследования является рассмотрение возможности и целесообразности применения целочисленного математического программирования для решения задач проектирования системы защиты информации объекта критической информационной инфраструктуры и размещения средств защиты на компонентах сети этого объекта. Для решения задачи предложено использовать методы математического программирования. Была разработана математическая модель, в которой на основании приказа ФСТЭК № 239 для каждого компонента объекта КИИ формируются наборы мер, которые должны быть выполнены, а для каждого средства защиты наборы мер, которые ими выполняются. В математической модели заданы ограничения, в соответствии с которыми каждая мера, актуальная для каждого компонента сети объекта, должна выполняться хотя бы одним средством защиты, которое установлено на данный компонент. Кроме этого, устанавливаются ограничения на ресурсы – объем оперативной памяти и дискового пространства. Целевая функция модели сводится к минимизации затрат на средства защиты при выполнении всех мер защиты для всех компонентов объекта. Математическая модель была реализована на языке Python 3.6 с использованием библиотеки Docplex. Полученные в ходе вычислительного эксперимента результаты свидетельствуют о том, что предложенный метод позволяет получить набор средств защиты, полностью выполняющий необходимые меры с минимизацией затрат, то есть оптимальный.

Ключевые слова: *информационная безопасность, система защиты, математическая модель, оптимизация, минимизация затрат*

Введение

К основным техническим средствам защиты информации можно отнести: антивирусы, межсетевые экраны, средства обнаружения вторжений [1]. Кроме них можно выделить средства защиты информации от несанкционированного доступа (СЗИ НСД), применение которых утверждено законодательно [2], DLP-системы, предназначенные для предотвращения утечки информации, инициированной сотрудниками самой организации [3], и SIEM-системы, задача которых – анализ данных, поступающих от других средств защиты информации [4].

Многие государства стали уделять внимание информационной безопасности и созданию нормативных документов, регламентирующих обеспечение информационной безопасности. В России такими документами стали федеральные законы № 149-ФЗ [5], № 152-ФЗ [6] и № 187-ФЗ [7], а также ряд других нормативных документов. Федеральный закон № 187 обязал все объекты критической инфраструктуры сообщать обо всех компьютерных инцидентах в специальный орган, отвечающий за реагирование на компьютерный инциденты (ГосСОПКА) [14]. Кроме федерального закона защите критической информационной инфраструктуры посвящен и приказ ФСТЭК № 239.

Приказ ФСТЭК № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» устанавливает следующие организационные и технические меры, которые должны обеспечивать информационную безопасность объекта критической информационной инфраструктуры: идентификация и аутентификация (ИАФ), управление доступом (УПД), ограничение программной среды (ОПС), защита машинных носителей информации (ЗНИ), аудит безопасности (АУД), антивирусная защита (АВЗ), предотвращение вторжений (компьютерных атак) (СОВ), обеспечение целостности (ОЦЛ), обеспечение доступности (ОДТ), защита технических средств и систем (ЗТС), защита информационной (автоматизированной) системы и ее компонентов (ЗИС), планирование мероприятий по обеспечению безопасности (ПЛН), управление конфигурацией (УКФ), управление обновлениями программного обеспечения (ОПО), реагирование на инциденты информационной безопасности (ИНЦ), обеспечение действий в нештатных ситуациях (ДНС), информирование и обучение персонала (ИПО) [8]. Большая часть этих мер должна выполняться с использованием средств защиты информации.

Подытоживая, можно сказать, что довольно распространенной задачей в области защиты информации являются выбор и установка средств защиты для обеспечения информационной бе-

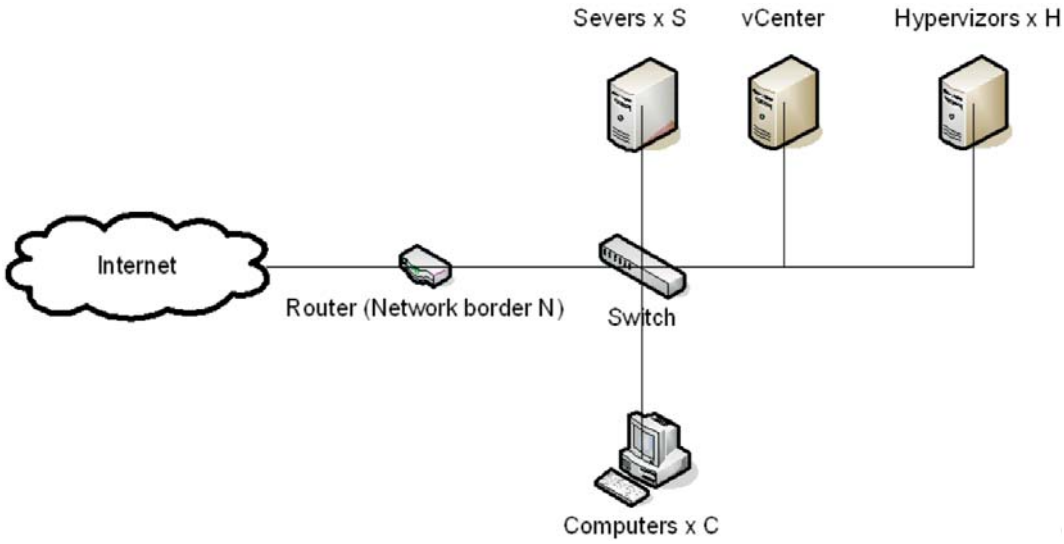

Рисунок. Обобщенная схема сети

зопасности корпоративной сети. При этом желательно, чтобы такие средства защиты информации, как антивирусы или СЗИ НСД, были одинаковыми на всех компьютерах сети, поскольку уже стало стандартом, что все средства защиты информации могут администрироваться с одного сервера администрирования [15].

Кроме того, довольно часто на машинах сети может оказаться программное обеспечение, несовместимое со средствами защиты, или ресурсы компьютера не позволяют разместить на нем то или иное средство защиты информации. В случае если компьютерная сеть организации включает несколько десятков или даже больше компьютеров, установка средств защиты становится нетривиальной задачей. Получить информацию о программном обеспечении, установленном на машинах сети, а также прочую информацию, которая может быть актуальна при решении подобной задачи, можно при помощи средств инвентаризации или контроля конфигураций [9]. Однако они не могут решить задачи выбора средств защиты и оценки возможности их применения в конкретной сети. В статье представлен подход, основанный на математическом программировании, которое хорошо показывает себя при решении задачи оптимизации [10].

Постановка задачи

Актуальными в настоящий момент являются задачи проектирования системы защиты информации для субъектов критической информационной инфраструктуры (КИИ). Каждому субъекту КИИ присваивается одна из категорий значимости. Всего три, третья – низшая [11].

Сеть субъекта может содержать компьютеры, серверы, гипервизоры, автоматизированные системы управления технологическими процессами, может быть подключена к Интернету. Обобщенная схема сети, при отсутствии АСУ ТП, может выглядеть, как на рисунке.

Для каждого компонента сети актуален некоторый набор мер. Необходимо осуществить выбор средств защиты информации таким образом, чтобы все меры были выполнены, а стоимость средств защиты была минимальной. В статье [12] предлагается составить модель для решения задачи проектирования системы защиты объекта КИИ, а также показаны модели. Мы же составим собственную, сводящуюся к решению оптимизационной задачи, поскольку этот подход считается целесообразным [13].

Математическая модель

Пусть K – количество компонентов сети объекта КИИ. M – количество всех мер, которые необходимо выполнить на данном объекте.

Введем вектор z_i (1):

$$z_i = \{z_1^i, z_2^i, ..., z_M^i\}, i = \overline{1..K}, \quad (1)$$

где $z_j^i = 1$, если j-я мера должна выполняться на компоненте i, и $z_j^i = 0$, если выполнение меры не обязательно.

Пусть D – количество средств защиты, рассматриваемых к установке на конкретном объекте критической информационной инфраструктуры.

Введем вектор d_l (2):

$$d_l = \{d_1^l, d_2^l, ..., d_M^l\}, l = \overline{1..D}, \quad (2)$$

где $d_j^l = 1$, если j-я мера выполняется l-м средством защиты, и $d_j^l = 0$, если мера не выполняется.

Введем также вектор установки средств защиты на компоненты объекта x_i (3):

$$x_i = \{x_1^i, x_2^i, ..., x_D^i\}, i = \overline{1..K}, \quad (3)$$

В соответствии с приказом ФСТЭК № 239 необходимо выполнить все актуальные для компонента i меры. Для этого наложим ограничение (4):

$$\sum_{l=1}^{D} x_l^i * d_j^l \geq i = \overline{1..K}, j = \overline{1..M}, \quad (4)$$

в соответствии с которым для каждого компонента i для каждой актуальной меры j должна выполняться установка хотя бы одного средства защиты, выполняющего данную меру.

Обозначим параметр c_l, которым выразим стоимость l-го средства защиты в рублях. Тогда сумма затрат для i-го компонента объекта составит (5):

$$P_i = \sum_{l=1}^{D} x_l^i * c_l. \quad (5)$$

Общие затраты для всех компонентов сети (6):

$$P^1 = \sum_{i=1}^{K} P_i. \quad (6)$$

При планировании установки средств защиты необходимо учитывать также ограниченность в ресурсах.

Модель с учетом ресурсных ограничений

Некоторые средства защиты требуют для размещения некоторого количества оперативной памяти и свободного дискового пространства. Обозначим параметры q_l и w_l, которыми обозначим требуемый объем оперативной памяти и свободного дискового пространства, измеряемые в мегабайтах, для установки l-го средства защиты. Также обозначим доступное количество оперативной памяти и дискового пространства на компоненте i параметрами φ_i и w_i (измеряются в мегабайтах).

Тогда можем ввести следующие ограничения: объем оперативной памяти, требуемый для установки всех необходимых средств защиты информации, должен быть меньше, чем доступный объем оперативной памяти на устройстве, на котором они устанавливаются (7):

$$\varphi_i - \sum_{l=1}^{D} x_l^i * q_l \geq 0, i = \overline{1..K}. \quad (7)$$

Аналогичное ограничение можно составить и для дискового пространства (8):

$$w_i - \sum_{l=1}^{D} x_l^i * w_l \geq 0, i = \overline{1..K}. \quad (8)$$

Однако возможна ситуация, когда доступного свободного пространства на диске или свободной оперативной памяти окажется недостаточно для того, чтобы разместить необходимые средства защиты на компоненте инфраструктуры. В этом случае необходимо произвести модернизацию – закупить дополнительный объем памяти.

Модель с добавлением памяти конечным устройствам

Обозначим переменные u_i и r_i, которыми выразим объем дополнительной оперативной памяти и дискового пространства (измеряется в мегабайтах), которые будут установлены на компоненты i. Зададим ограничение, согласно которому общий объем оперативной памяти на компоненте i с установкой дополнительных модулей и средств защиты должен быть неотрицательным (9):

$$\varphi_i + u_i - \sum_{l=1}^{D} x_l^i * q_l \geq 0, i = \overline{1..K}. \quad (9)$$

Аналогичное ограничение можно составить и для дискового пространства. Ограничение примет вид (10):

$$w_i + r_i - \sum_{l=1}^{D} x_l^i * w_l \geq 0, i = \overline{1..K}. \quad (10)$$

Обозначим параметры c_i^u и c_i^r, выражающие цену оперативной памяти и дискового пространства, устанавливаемых на компоненте i. Тогда общая стоимость за оперативную память и дисковое пространство составит (11):

$$P^2 = \sum_{i=1}^{K} c_i^u * u_i + c_i^r * r_i. \quad (11)$$

Целевая функция всей задачи сводится к минимизации всех затрат (12):

$$P^1 + P^2 \to \min. \quad (12)$$

Поскольку задача свелась к задаче линейного целочисленного программирования, для реализации математической модели была написана компьютерная программа на языке Python 3.6 с использованием библиотеки Docplex.

Алгоритм проектирования системы безопасности

Для того чтобы воспользоваться предложенным методом, предлагается осуществить следующий порядок действий.

1. Определить состав компонентов объекта, то есть K.

2. Определить категорию объекта КИИ в соответствии с постановлением о категорировании № 127 [12].

3. В зависимости от категории определяется базовый набор мер, которые должны выполняться

Таблица 1. Компоненты сети объекта

Автоматизированное рабочее место			
Название	Операционная система	Свободное ОЗУ (Мб)	Свободное дисковое пространство (Мб)
АРМ0	Windows 7	7781	37637
АРМ1	Windows 8	6844	860529
АРМ2	Windows 8	4453	326865
АРМ3	Windows 8	6416	462265
АРМ4	Windows 7	2024	746431
АРМ5	Windows 10	6205	653703
АРМ6	Windows 8	1437	358888
АРМ7	Windows 8	1026	376002
АРМ8	Windows 7	7654	457823
АРМ9	Windows 8	6197	179511
АРМ10	Windows 10	2192	377344
АРМ11	Windows 8	6671	521337
АРМ12	Windows 8	4346	675906
АРМ13	Windows 7	4959	25700
АРМ14	Windows 7	3707	155854
АРМ15	Windows 8	6233	404572
АРМ16	Windows 8	8	165055
АРМ17	Windows 7	6517	737081
АРМ18	Windows 7	3714	681141
АРМ19	Windows 8	5874	62372

Сервер	
Название	Операционная система
Сервер0	Ubuntu 16
Сервер1	Windows Server 2012
Сервер2	Windows Server 2019
Сервер3	Windows Server 2012
Сервер4	Windows Server 2012
Сервер5	Windows Server 2012
Сервер6	Windows Server 2016
Гипервизор ESXi	2
Сервер управления vCenter	1
Внешняя граница сети	1

для объекта, этот набор мер затем уточняется и адаптируется. В результате должен получиться набор мер M, который должен быть определен для каждого компонента сети.

4. Сформировать список средств защиты D, для каждого из которых должен быть определен набор выполняемых мер d_l из приказа ФСТЭК № 239 и должны быть известны ресурсные ограничения q_l, w_l и стоимость c_l.

5. Задать переменные оперативной памяти u_i и жестких дисков r_i для каждого компонента, для которого это актуально. Также указать их стоимости c_i^u, c_i^r.

6. Загрузить параметры в программу и произвести расчет.

Если модель разрешима, в результате будет получен оптимальный набор средств, необходимый и достаточный для выполнения всех мер защиты информации, актуальных для объекта КИИ.

Вычислительный эксперимент

Пусть у нас имеется объект КИИ 3-й категории в составе 20 компьютеров, 7 серверов, 2 гипервизоров, сервера управления виртуализацией vCenter, имеющий доступ к сети Интернет (таблица 1).

Таблица 2. Меры КИИ 3-й категории

Автоматизированное рабочее место	ИАФ (1,2,3,4,7) УПД (1,2,4,6,10,11), ЗНИ: (1,5,7,8), АУД (4,6,7,10), АВЗ (1,2,4), ЗИС (1), ИНЦ (1,2,3,6) УКФ (3)
Сервер	ИАФ (1,2,3,4,7), УПД (1,2,4,6,10,11), ЗНИ (1,5,7,8), АУД (4,6,7,10), АВЗ (1,2,4), (ЗИС 1), ИНЦ (1,2,3,6), УКФ (3)
Гипервизор	ИАФ (1,2,3,4,7), УПД (1,2,4,6,10,11,12), ЗНИ (5,6,7), АУД (3,4,6,7,8,10), ЗИС (1,2,4,6,13,19,20,27,39), ИНЦ (1,2,3,6), УКФ (3), ДНС (4,5),
Граница сети	ИАФ (1,2,3,4,7), УПД (1,2,4,6,10,11), АУД (3,4,6,7,8,10), ЗИС (2,5,6,8,19,20,34,35), ИНЦ (1,2,3,6), УКФ (3), ДНС (5)

Таблица 3. Средства защиты информации

Антивирусы				
Kaspersky Endpoint Security 10	Windows (7,8,10), Windows Server (2008, 2012, 2016, 2019)	2048	2048	АВЗ (1,2,3,4)
Kaspersky Endpoint Security 10 Linux	Ubuntu (14,16), Centos (7), Debian (7, 8)	2048	1500	АВЗ (1,2,3,4)
Dr. Web 11	Windows (7,8,10), Windows Server (2008, 2012, 2016, 2019)	4096	8192	АВЗ (1,2,3,4)
Dr.Web Linux	Debian (7,8,9), Fedora (27,28,29), Ubuntu (14,16,18)	1024	512	АВЗ (1,2,3,4)
СЗИ НСД				
Название	Поддерживаемые операционные системы	ОЗУ (Мб)	Дисковое пространство (Мб)	Выполняемые меры
Secret Net Studio	Windows (7,8,10), Windows Server (2008, 2012, 2016, 2019)	2048	4096	ИАФ (1,2,3,4,6,7), УПД (1,2,4,6,7,10,11,12), ЗНИ (1,4,5,6,7,8), АУД (4,5,6,7,8,9,10), ЗИС (1,4,10,13,18 ,20,21,23,27,33,34,35,37), ИНЦ (1,2,3,6), УКФ (3), ДНС (5)
Secret Net LSP	Centos (7), Debian (9), Ubuntu (18)	512	600	ИАФ (1,2,3,4,7), УПД (1,2,4,6,11,12), ЗНИ (1,7,8), АУД (4,6,7,8,9,10), ЗИС (1,10,13,20,23,33), ИНЦ (1,2,3,6), УКФ (3)
Dallas Lock 8.0	Windows (7,8,10), Windows Server (2008, 2012, 2016, 2019)	2048	4096	ИАФ (1,2,3,4,6,7), УПД (1,2,4,6,7,10, 11,12), ЗНИ (1,4,5,6,7,8), АУД (4,5,6, 7,8,9,10), ЗИС (1,4,10,13,18,20, 21,23,27,33,34,35,37). ИНЦ (1,2,3,6), УКФ (3), ДНС (5)
Dallas Lock Linux	Centos (7), Debian (8), Ubuntu (16), Fedora (24)	512	1500	ИАФ (1,2,3,4,7), УПД (1,2,4,6,10,11,12), ЗНИ (1,7,8), АУД (4,6,7,8,9,10), ЗИС (1,10,13,20, 23,33), ИНЦ (1,2,3,6), УКФ (3)
Защита виртуализации				
vGate		ИАФ (1,2,3,4,6,7), УПД (1,2,3,4,6,10,11,12), ЗНИ (5,6,7), АУД (3,4,6,7,8,9,10), ЗИС (1,2,4,6,13,19,20,27,37,39), ИНЦ (1,2,3,6), УКФ (1,2,3,4), ДНС (4,5)		
СЗИ ВИ Dallas Lock		ИАФ (1,2,3,4,6,7), УПД (1,2,3,4,6,10,11,12), ЗНИ (5,6,7), АУД (3,4,6,7,8,9,10), ЗИС (1,2,4,6,13,19,20,27,37,39), ИНЦ (1,2,3,6), УКФ (1,2,3,4), ДНС (4,5)		

Окончание таблицы 3

Защита сетевой инфраструктуры	
VipNet Coordinator	ИАФ (1,2,3,4,6,7), УПД (1,2,3,4,6,10,11,12), ЗНИ (5,6,7), АУД (3,4,6,7,8,9,10), ЗИС (1,2,4,5,6,8,11,18,19,20,27,31,32,34,35), ИНЦ (1,2,3,6), ДНС (5)
АПКШ Континент	ИАФ (1,2,3,4,6,7), УПД (1,2,3,4,6,10,11,12), ЗНИ (5,6,7), АУД (3,4,6,7,8,9,10), ЗИС (1,2,4,5,6,8,11,18,19,20,27,31,32,34,35), ИНЦ (1,2,3,6), ДНС (5)

Таблица 4. Решение без учета ограничений

КИИ 3-й категории	
АРМ 0-19	Dallas Lock 8.0, Dr. Web 11
Сервер 0	Dallas Lock Linux, Dr. Web Linux
Серверы 1-6	Dallas Lock 8.0, Dr. Web 11
Средства администрирования	Dr.Web Центр Управления, Dallas Lock 8.0 Server, Dallas Lock СЗИ ВИ Сервер безопасности
Гипервизор 0,1	Dallas Lock ВИ ESXi
vCenter	Dallas Lock vCenter
Граница сети	ViPNet Coordinator HW100

Таблица 5. Решение с учетом ограничений

КИИ 3-й категории	
АРМ 2,4,6,7,10,12,13,14,16,18,19	Не удалось установить средства защиты
АРМ 1,3,5,8,9,11,15,17	Dallas Lock Linux, Dr. Web 11
Сервера 0	Dallas Lock Linux, Dr.Web Linux
Серверы 1-6	Dallas Lock 8.0, Dr. Web 11
Средства администрирования	Dr.Web Центр Управления, Dallas Lock 8.0 Server, Dallas Lock СЗИ ВИ Сервер безопасности
Гипервизор 0,1	Dallas Lock ВИ ESXi
vCenter	Dallas Lock vCenter
Граница сети	ViPNet Coordinator HW100

Примем, что для них актуальны следующие меры в соответствии с приказом ФСТЭК № 239 (таблица 2).

Сформируем состав средств защиты информации, сертифицированных ФСТЭК, которые могут применяться для защиты объекта КИИ (таблица 3).

Решение задачи без учета ограничений в ресурсах

При решении задачи без учета ограничений в ресурсах для выполнения необходимых мер будут задействоваться следующие средства защиты (таблица 4), общая стоимость средств защиты – 927 600 рублей.

Решение задачи с учетом ограничений в ресурсах

Попробуем решить задачу, используя ограничения по оперативной памяти и дисковому пространству (таблица 5). Успешно установить средства защиты информации на все компоненты сети не удалось. Общая цена установленных средств защиты составила 641 600 рублей.

Решение задачи с добавлением памяти конечным устройствам

Теперь смоделируем решение задачи, при котором возможна модернизация компонентов сети (таблица 6). Общая стоимость установки средств защиты и модернизации компонентов сети – 989 230 рублей.

Для успешного решения задачи были использованы дополнительные ресурсы. Кроме того, для сервера 0 не выполняется требование ЗНИ5 (Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации), это объясняется тем, что СЗИ НСД для операционных систем Linux не выполняют эту меру. Для того чтобы эту меру

Таблица 6. Решение с добавлением памяти

КИИ 3-й категории	
АРМ 0-19	Dallas Lock 8.0, KES 11
Сервера 0	Dallas Lock Linux, Kasp. Linux
Сервер 1-6	Dallas Lock 8.0, KES 11
Средства администрирования	Dr.Web Центр Управления, Dallas Lock 8.0 Server, Dallas Lock СЗИ ВИ Сервер безопасности
Гипервизор 0,1	Dallas Lock ВИ ESXi
vCenter	Dallas Lock vCenter
Граница сети	ViPNet Coordinator HW100
Дополнительные ресурсы	
Название	Дополнительные ресурсы
АРМ4	3072 МБ оперативной памяти
АРМ6	3072 МБ оперативной памяти
АРМ7	3072 МБ оперативной памяти
АРМ10	2048 МБ оперативной памяти
АРМ14	1024 МБ оперативной памяти
АРМ16	4096 МБ оперативной памяти
АРМ18	1024 МБ оперативной памяти

все-таки выполнить, можно переустановить операционную систему на данный сервер либо воспользоваться организационными мерами.

Выводы

Предложенный метод расчета средств защиты информации на объектах КИИ призван помочь в решении задачи обеспечения информационной безопасности при осуществлении выбора средств защиты. Он может быть довольно полезен в случае, когда объект критической информационной инфраструктуры включает в себя множество АРМ и серверов, что делает анализ возможности размещения средств защиты чрезвычайно трудоемкой задачей.

В данной работе не были рассмотрены автоматизированные системы управления технологическими процессами, однако расширение модели и включение в нее АСУ ТП возможно. Для этого необходимо определить меры, которые нужно выполнить на конкретных устройствах, доступные ресурсы этих устройств, а также определить средства защиты, выполняющие меры защиты, требования ресурсов средств защиты и задать соответствующие ограничения.

Литература

1. Веретенников А. Классификация средств защиты информации от ФСТЭК и ФСБ России. URL: https://www.anti-malware.ru/analytics/Market_Analysis/infosecurity-systems-classification-fsb-fstek#part5 (дата обращения: 23.03.2020).
2. Основные подсистемы защиты информации от несанкционированного доступа и особенности их настройки / А.А. Герасимов [и др.] // Инженерный журнал: наука и инновации. 2013. № 11 (23). URL: http://engjournal.ru/catalog/it/security/1017.html (дата обращения: 24.03.2020).
3. Киздермишов А.А., Киздермишова С.Х. К вопросу о вводе в эксплуатацию DLP-систем // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2017. № 3 (206). С. 128–133.
4. Кириллов В.А., Касимова А.Р., Алёхин А.Д. Система сбора и корреляции событий (siem) как ядро системы информационной безопасности // Вестник Казанского технологического университета. 2016. № 13. С. 132–134.
5. Каретников М.К. Защита информации в нормах федерального закона Российской Федерации // Спецтехника и связь. 2013. № 1. С. 52–57.
6. Чуб В.С. Анализ литературы и нормативно-правовой базы в области защиты персональных данных // Инновационная наука. 2017. № 11. С. 55–59
7. Талипова Л.Р. Концептуальные основы правовой регламентации критической информационной инфраструктуры в Российской

Федерации // Гуманитарные, социально-экономические и общественные науки. 2018. № 5. С. 216–218.
8. Витенбург Е.А., Левцова А.А. Выбор элементов комплекса защиты информационной системы предприятия на основе требований нормативно-правовых документов // Advanced Engineering Research. 2018. № 3. С. 333–338.
9. Рябов. А. Обзор Efros Config Inspector. URL: https://www.anti-malware.ru/reviews/Efros-Config-Inspector (дата обращения: 23.03.2020).
10. Картак В.М., Башмаков Н.М. Оптимизация размещения видеокамер // Вопросы защиты информации. 2019. № 4 (127). С. 54–58.
11. Щелкин К.Е., Звягинцева П.А., Селифанов В.В. Возможные подходы к категорированию объектов критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2019. № 1. С. 128–133.
12. Шабуров А.С., Зонова В.Э. Модель реализации требований по защите информации объектов критической информационной инфраструктуры // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. 2019. № 32. С. 130–147.
13. Шабуров А.С., Миронова А.А. О повышении эффективности защиты персональных данных в информационных системах открытого типа // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. 2015. № 16. С. 106–117.
14. Горелик В.Ю., Безус М.Ю. О безопасности критической информационной инфраструктуры Российской Федерации // StudNet. 2020. № 9. С. 1438–1448.
15. Ляшко Д.А., Аникин И.В. Моделирование агента и менеджера системы удаленного администрирования средствами защиты информации от несанкционированного доступа // Известия ЮФУ. Технические науки. 2012. № 12 (137). С. 96–104.

Получено 11.10.2021

Картак Вадим Михайлович, д.ф-м.н, профессор, заведующий кафедрой Вычислительной Техники и Защиты Информации (ВТиЗИ) Уфимского Государственного Авиационного Технического Университета (УГАТУ). 450008, Республика Башкортостан, г. Уфа, ул. К. Маркса, д. 12. Тел +7 917 433-39-19. E-mail: KVmail@mail.ru

Башмаков Наиль Маратович, аспирант кафедры ВТиЗИ УГАТУ. 450008, Республика Башкортостан, г. Уфа, ул. К. Маркса, д. 12. Тел. +7 917 763-82-04. E-mail: nail.bashmakov@gmail.com

THE APPLICATION OF MATHEMATICAL PROGRAMMING FOR SOLVING THE PROBLEM OF DESIGNING THE PROTECTION SYSTEM OF THE OBJECT OF CRITICAL INFRASTRUCTURE

Kartak V.M., Bashmakov N.M.
Ufa State Aviation Technical University, Ufa, Russian Federation
E-mail: KVmail@mail.ru, nail.bashmakov@gmail.com

The possibility and practicability of using integer mathematical programming for solving problems of designing an information protection system for an object of a critical information infrastructure and placing protection tools on the components of this object is investigated. A mathematical model was developed, in which, based on FSTEC order No. 239, sets of measures are formed for each component of the object of a critical information infrastructure, which must be performed, and for each protection tool, sets of measures that are performed by them. In the mathematical model, constraints are set, according to which each measure that is relevant for each component of the object's network must be performed by at least one mean of protection that is installed on this component. In addition, resource limits are set – the amount of RAM and disk space. The objective function of the model comes down to minimizing the cost of security tools while implementing all security measures for all components of the object. The mathematical model was implemented in Python 3.6 using the Docplex library. The results of the computational experiment indicate that the proposed method allows to obtain a set of protection tools that fully fulfill the necessary measures with minimizing costs, that is, optimal.

Keywords: *mathematical programming, critical information infrastructure, information security, security system, mathematical model, optimization, cost minimization*

DOI: 10.18469/ikt.2021.19.4.03

Kartak Vadim Mihajlovich, Ufa State Aviation Technical University, 12, K. Marx Street, Ufa, 450008, Russian Federation; Doctor of Physics and Mathematics. Tel. +7 917 433-39-19. E-mail: KVmail@mail.ru

Bashmakov Nail Maratovich, Ufa State Aviation Technical University, 12, K. Marx Street, Ufa, 450008, Russian Federation. Tel. +7 917 763-82-04. E-mail: nail.bashmakov@gmail.com

References

1. Veretennikov A. Classification of information security tools from the FSTEC and the FSB of Russia. URL: https://www.anti-malware.ru/analytics/Market_Analysis/infosecurity-systems-classification-fsb-fstek#part5 (accessed: 23.03.2020). (In Russ.)
2. Gerasimov A.A. et al. The main subsystems for protecting information from unauthorized access and features of their settings. *Inzhenernyj zhurnal: nauka i innovatsii*, 2013, no. 11 (23). URL: http://engjournal.ru/catalog/it/security/1017.html (accessed: 24.03.2020). (In Russ.)
3. Kizdermishov A.A., Kizdermishova S.H. On the issue of commissioning DLP systems. *Vestnik Adygejskogo gosudarstvennogo universiteta. Serija 4: Estestvenno-matematicheskie i tehnicheskie nauki*, 2017, no. 3 (206), pp. 128–133. (In Russ.)
4. Kirillov V.A., Kasimova A.R., Alehin A.D. System of collection and correlation of events (siem) as the core of the information security system. *Vestnik Kazanskogo tehnologicheskogo universiteta*, 2016, no. 13, pp. 132–134. (In Russ.)
5. Karetnikov M.K. Information protection in the norms of the federal law of the Russian Federation. *Spetstehnika i svjaz'*, 2013, no. 1, pp. 52–57. (In Russ.)
6. Chub V.S. Analysis of literature and regulatory framework in the field of personal data protection. *Innovatsionnaja nauka*, 2017, no. 11, pp. 55–59. (In Russ.)
7. Talipova L.R. Conceptual framework for legal regulation of critical information infrastructure in the Russian Federation. *Gumanitarnye, sotsial'no-ekonomicheskie i obschestvennye nauki*, 2018, no. 5, pp. 216–218. (In Russ.)
8. Vitenburg E.A., Levtsova A.A. Selection of elements of the enterprise information system protection complex based on the requirements of regulatory documents. *Advanced Engineering Research*, 2018, no. 3, pp. 333–338. (In Russ.)
9. Ryabov A. Review of Efros Config Inspector. URL: https://www.anti-malware.ru/reviews/Efros-Config-Inspector (accessed: 23.03.2020).
10. Kartak V.M., Bashmakov N.M. Camera Placement Optimization. *Voprosy zaschity informatsii*, 2019, no. 4 (127), pp. 54–58. (In Russ.)
11. Schelkin K.E., Zvjagintseva P.A., Selifanov V.V. Possible approaches to the categorization of critical information infrastructure objects. *Interekspo Geo-Sibir'*, 2019, no. 1, pp. 128–133. (In Russ.)
12. Shaburov A.S., Zonova V.E. Model for implementing information protection requirements for critical information infrastructure objects. *Vestnik PNIPU. Elektrotehnika, informatsionnye tehnologii, sistemy upravlenija*, 2019, no. 32, pp. 130–147. (In Russ.)
13. Shaburov A.S., Mironova A.A. On improving the efficiency of personal data protection in open type information systems. *Vestnik PNIPU. Elektrotehnika, informatsionnye tehnologii, sistemy upravlenija*, 2015, no. 16, pp. 106–117. (In Russ.)

14. Gorelik V.Yu., Bezus M.Yu. On the security of the critical information infrastructure of the Russian Federation. *StudNet*, 2020, no. 9, pp. 1438–1448. (In Russ.)
15. Ljashko D.A., Anikin I.V. Modeling the agent and manager of the remote administration system by means of protecting information from unauthorized access. *Izvestija YuFU. Tehnicheskie nauki*, 2012, no. 12 (137), pp. 96–104. (In Russ.)

Received 11.10.2021

УДК 004.89

АДАПТАЦИЯ МЕХАНИЗМОВ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ ДЛЯ КООПЕРАТИВНОГО ПРОТИВОСТОЯНИЯ УГРОЗАМ ВТОРЖЕНИЯ В АВТОНОМНЫЕ ИНФОТЕЛЕКОММУНИКАЦИОННЫЕ ОБЪЕКТЫ

Скатков А.В., Моисеев Д.В., Брюховецкий А.А.
Севастопольский государственный университет, Севастополь, РФ
E-mail: dmitriymoiseev@mail.ru

В настоящей работе продолжены исследования авторов, посвященные адаптации механизмов искусственных иммунных систем путем модификации классических математических моделей в соответствии со спецификой искусственных иммунных систем, что позволило значительно повысить их эффективность при выполнении прогнозирования состояния объекта контроля – решении задачи идентификации, которая заключается в нахождении мощностей источников деградации ресурсов (вирусной атаки) автономной инфотелекоммуникационной системы по имеющимся экспериментальным данным. В работе предложены модели кооперативного взаимодействия нескольких автономных инфотелекоммуникационных систем, защита которых построена на базе искусственных иммунных систем. Как известно, в настоящее время множество методов, основанных на принципах иммунологии, расширяется, а искусственные иммунные системы вызывают наибольший интерес среди исследователей благодаря свойствам особых механизмов памяти, поиска, распознавания, адаптации и др. В работе впервые предлагается использование механизмов передачи антивирусных баз между искусственной иммунной системой донора и искусственной иммунной системой акцептора. Получены результаты вычислительного эксперимента, свидетельствующие о потенциальной эффективности предлагаемых алгоритмов.

Ключевые слова: *искусственный интеллект, беспилотное средство контроля, искусственные иммунные системы, кооперативные системы*

Введение

Бурное развитие в настоящее время теории и систем искусственного интеллекта (ИИ) и построенных с его использованием автономных беспилотных транспортных средств (БТС) требует уделять большое внимание вопросам защиты информации (ЗИ), накапливаемой, хранимой и обрабатываемой в информационных системах (ИС), которыми и являются БТС [1; 2]. Особую роль в ЗИ БТС занимают вопросы создания систем превентивной ЗИ [3].

Как известно, применение различных эвристических алгоритмов, вдохновленных живой природой, – методов муравьиных колоний, роевого интеллекта, искусственных нейронных сетей, имитации отжига, эволюционные алгоритмы и т. д., используется в первую очередь для решения задач оптимизации [4; 5].

Одним из актуальных классов биоинспирированных алгоритмов в современных исследованиях являются иммунные системы. Методы иммунных систем, ориентированные на решение задачи глобальной оптимизации, основаны на некоторых аспектах поведения иммунной системы человека в процессе защиты ею организма. Защитные клетки иммунной системы (антитела) претерпевают при этом множество изменений, целью которых является создание клеток, обеспечивающих наилучшую защиту. Искусственные иммунные системы (ИИС) обладает основными свойствами искусственного интеллекта: памятью, способностью к обучению и принятию решений в незнакомой ситуации [6; 7].

В работах по биологии и медицине иммунные системы представляют собой сложнейшие децентрализованные системы, способные решать задачу обеспечения жизнедеятельности организма в условиях агрессивной, все время меняющейся окружающей среды [8–11].

В настоящей работе продолжены исследования авторов, начатые в [12] и посвященные адаптации механизмов искусственных иммунных