УДК 004.056+004.051+004.89 DOI: 10.26102/2310-6018/2020.30.3.022

Модель оценки эффективности конфигурации системы защиты информации на базе генетических алгоритмов

И.М. Космачева, Н.В. Давидюк, И.В. Сибикина, И.Ю. Кучин
Федеральное государственное бюджетное учреждение высшего образования «Астраханский государственный технический университет», Астрахань, Российская Федерация

Резюме: В статье представлена иерархическая структура настроек средств защиты информации, введены критерии оценки эффективности систем защиты, формализовано понятие «конфигурация системы защиты» на базе объектов эволюционного моделирования, таких как популяция, хромосома (вектор решения), функция пригодности решения, и т.д. Разработана математическая модель для построения системы защиты с применением методов искусственного интеллекта. Предлагаемая система отличается возможностью учета влияния случайных факторов (квалификация обслуживающего персонала, отказы техники, время атаки на систему защиты) при выборе варианта защиты и возможностью адаптации системы защиты под изменяющиеся условия среды. Такая модель позволит использовать ее не только в профессиональной деятельности специалистов по информационной безопасности, но и в учебной в качестве своеобразного тренажера. Разработка эффективной системы защиты с использованием генетического алгоритма возможна на основе данных мониторинга событий в системе, данных, полученных от экспертов и в ходе имитационного моделирования работы системы защиты. Таким образом, результаты исследования имеют прикладной характер и могут быть использованы в разработках, связанных с проектированием информационных систем, систем поддержки принятия решений в сфере информационной безопасности.

Ключевые слова: эволюционное моделирование, имитационное моделирование, генетический алгоритм, угрозы информационной безопасности, средства защиты информации, конфигурация системы защиты, защита данных.

Для цитирования: Космачева И.М., Давидюк Н.В., Сибикина И.В., Кучин И.Ю. Модель оценки эффективности конфигурации системы защиты информации на базе генетических алгоритмов. *Моделирование, оптимизация и информационные технологии.* 2020;8(3). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/08/KosmachevaSoavtors_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.022.

The model for evaluating the effectiveness of an information security system configuration based on genetic algorithms

I.M. Kosmacheva, N.V. Daviduyk, I.V. Sibikina, I.Y. Kuchin
Federal State Budget Educational Institution of Higher Education "Astrakhan State Technical University", Astrakhan, Russian Federation

Abstract: The article presents the hierarchical structure of settings for information security tools, introduced criteria for evaluating the effectiveness of security systems, formalizes the concept of “security system configuration” based on evolutionary modeling objects, such as population,

chromosome (solution vector), fitness function, etc. The mathematical model for constructing a security system using artificial intelligence methods has been developed. The proposed system is characterized by the possibility of considering the influence of random factors (staff, equipment failures, attack time on the security system) when choosing a protection option and the ability of adapting the protection system to changing environmental conditions. This model allows to use it not only in the professional activities of information security specialists, but also in training process as a kind of simulator. The development of an effective information security system using a genetic algorithm is possible on the basis of system monitoring events data, data received from experts and during simulation of the protection system. Thus, the research results have an applied nature and can be used in developments related to the design of information systems, decision support systems in the field of information security.

Keywords: evolutionary modeling, simulation, genetic algorithm, threats to information security, information security tools, security system configuration, data protection.

For citation: Kosmacheva I.M., Davidyuk N.V., Sibikina I.V. , Kuchin I.Y. A model for evaluating the effectiveness of information security system configuration based on genetic algorithms. *Modeling, Optimization and Information Technology*. 2020;8(3). Available from: https://moit.vivt.ru/wp-content/uploads/2020/08/KosmachevaSoavtors_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.022 (In Russ).

Введение

Надежное функционирование и эффективность системы защиты определяется вероятностью нейтрализации системой защиты информации (СЗИ) угроз информационной безопасности (ИБ), источниками которых являются умышленные действия заинтересованных лиц, технические сбои и ошибки сотрудников, связанные, в том числе, и небезопасными настройками системы. Эффективность СЗИ со временем меняется вместе с изменениями в IT-инфраструктуре, необходимо оперативно определять моменты управляющих воздействий, связанные со сменой одного решения по защите на другое. Оценить вероятность угроз и ущерб, зависящий сразу от совокупности факторов и их сочетаний, математически сложно. Для этого необходимо разрабатывать современные математические модели оценки защищенности информационной системы (ИС) при текущей конфигурации СЗИ, отличающиеся от распространенного подхода на базе профилей защиты.

В популярных методиках оценка эффективности СЗИ базируется на использовании стандартов, нормативных документов [1-5] и сопоставлении требований и параметров защиты. Зарегулированность процесса построения системы защиты позволяет атакующим прогнозировать типовые конфигурации СЗИ, что облегчает проведение атак на систему. К тому же при таком подходе излишне усложняется и удорожается СЗИ.

Атаки же становятся все сложнее, число уникальных киберинцидентов продолжает увеличиваться - средний прирост 34% [6, 7]. Методы реализации угроз информационной безопасности постоянно эволюционируют, для атак используются технологии искусственного интеллекта. Развитие IT-технологий приводит к необходимости чаще пересматривать текущие модели СЗИ, адаптировать их под изменяющиеся условия внешней среды на базе методов искусственного интеллекта, оптимизации, нечеткой логики, машинного обучения. Таким образом, актуальна проблема эволюционного развития систем информационной безопасности. И, в связи с этим, применение методов имитационного и эволюционного моделирования, как инструмента выбора оптимального решения по защите данных, наиболее предпочтителен.

Постановка задачи моделирования

Развитие автоматизированных систем по считыванию настроек и параметров работы ИС, систем защиты СЗ создают предпосылки к разработке систем защиты, конфигурация которых бы в динамическом режиме оптимизировалась на основе обрабатываемой информации о событиях в системе.

Сложность тестирования выбранной конфигурации СЗ для оценки ее эффективности из-за недостатка у организации ресурсов (материальных, временных, людских) заставляет обращаться к мнению экспертов, которое не всегда объективно или быстро устаревает. Многочисленные сочетания параметров работы СЗИ могут по-разному сказываться на событиях в системе, и как именно, не всегда знает даже высококлассный специалист. Данные, связывающие вариант конфигурации системы защиты с устойчивостью ее к атакам и сбоям, необходимо эффективнее использовать для принятия решений в сфере защиты.

Для решения этой задачи определим понятие “конфигурация” системы защиты информации как вектор значений настроек и правил защиты. Далее на основе заданных параметров защиты и параметров среды в имитационной модели проигрываются случайные события для оценки устойчивости СЗИ к возможным угрозам. При этом может использоваться, например, статистика сбоев серверного оборудования, загрузки зловредного вложения пользователями и др. С помощью имитационной модели можно варьировать события в системе защиты, учитывать бихевориальные характеристики (поведенческие особенности) технического персонала. Такие события как увольнение администратора безопасности, повышение квалификации, нарушение политик информационной безопасности могут влиять на уровень защищённости системы и учтены при имитационном моделировании.

В результате применения имитационного моделирования можно оценить вероятность, время простоя каждого узла сети или их комбинации в случае успешной реализации атаки, а также другие показатели, от которых зависит эффективность системы защиты при заданной конфигурации и учесть при расчете комплексной оценки. Т.о., формируется база конфигураций СЗИ и значений их функции пригодности. Эти решения можно использовать как начальная популяция, на базе которой будет осуществляться формирование новых решений для оценки и поиска оптимального варианта на базе методов оптимизации.

Анализ методов оптимизации

В рамках исследования для автоматизации поиска был проведен анализ классических и эвристических методов оптимизации, результаты которого обобщены в Таблице 1.

Генетические алгоритмы (ГА) – это метод решения оптимизационных задач, основанный на биологических принципах естественного отбора и эволюции, моделирующий «выживание» наиболее приспособленных к условиям среды объектов (вариантов защиты, др.). Под решением с точки зрения биологической аналогии в данном случае понимается хромосома.

Таблица 1 -Сравнительный анализ методов оптимизации
Table 1-Comparative analysis of optimization methods

Методы оптимизации (выбора)	Особенности
Методы математической статистики	• основываются на сборе, накоплении и систематизации статистических данных о решении; • необходимо знание не только выборочного среднего значения решения, но и разброс значений около выборочного среднего.
Классические методы многокритериальной оптимизации	• используется для исследования процессов по результатам экспериментов на математической модели с неслучайными (детерминированными) переменными • целевая функция должна быть задана аналитическим путем; • применение метода зависит от возможности дифференцирования функции и числа переменных; • с ростом размерности задачи резко снижается эффективность метода.
Эвристические методы оптимизации (генетический алгоритм)	• может применяться для решения сложных, неформализованных задач, для которых не разработано специальных методов; • применим для поиска «достаточно хорошего» решения задачи за «достаточно короткое время»; • имеет преимущества перед другими алгоритмами при очень больших размерностях задач и отсутствия упорядоченности в исходных данных, когда альтернативой им является метод полного перебора вариантов; • поиск решения основан на оптимизации случайно заданного множества решений, что позволяет анализировать одновременно несколько путей.

В результате анализа поставленной проблемы для поиска оптимальной конфигурации СЗИ предлагается использовать генетический алгоритм как имеющий преимущества [8-11] в том, что он может применяться для решения сложных, неформализованных задач произвольной размерности, а новые решения в нем синтезируются на основе старых, т.е. происходит эволюционное развитие оптимальных решений.

Результаты

Формализация задачи

Особи, входящие в популяцию, в генетических алгоритмах представляются хромосомами с закодированным в них множествами параметров задачи, т.е. решений, которые иначе называются точками в пространстве поиска. Хромосома - объект, строка, последовательность, упорядоченная последовательность генов. Ген (свойство, параметр, признак, характеристика) – это атомарный элемент генотипа, в частности, хромосомы.

Пусть конфигурация системы защиты информации (вектор h, хромосома) хранит информацию о включении или невключении защитной меры (настройки СЗ). Вектор h имеет размерность n, n- количество защитных мер. Их число может быть различным,

возможные варианты можно проанализировать на основе классификации СЗИ. В результате было построено иерархическое дерево всевозможных настроек средств защиты информации, которые могут использоваться в системе. Узлы второго уровня дерева получены на основе классификации СЗИ в соответствии с требованиями и руководящими документами ФСТЭК. На третьем уровне иерархии в соответствии с рисунком 1 расположены наиболее популярные сертифицированные СЗИ. На четвертом уровне располагается перечень их настроек, а на пятом уровне – значения настроек (на рисунке не отображены из-за громоздкости дерева).

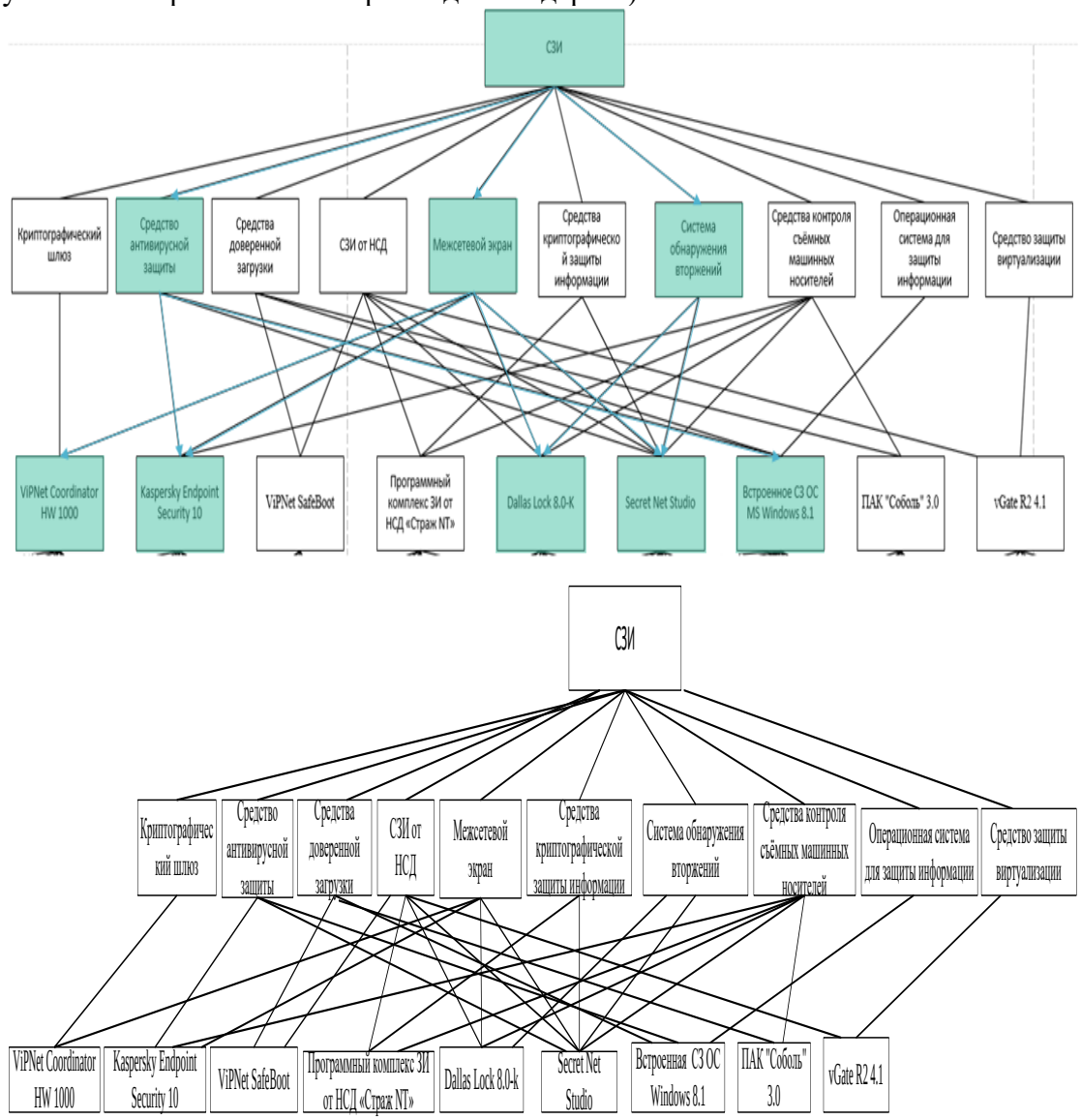

Рисунок 1 -Дерево настроек средств защиты информации
Figure. 1 -Information security settings tree

Список возможных общих настроек, расположенных на четвертом уровне, может включать:

1. Проверка на наличие вредоносных программ, которые зарегистрированы в базе сигнатур (применяется настройка средствами защиты KasperskyEndpointSecurity 10, SecretNetStudio).
2. Назначение дополнительных IP-адресов.
3. Организация обработки трафика из нескольких VLAN.
4. Фильтрация трафика виртуальных машин и др.

При желании возможно увеличение числа и дальнейшая декомпозиция на более “детализированные” настройки, увеличение количества используемых средств защиты и задание другой структуры дерева.

Для выявления оптимальных настроек могут использоваться схемы защиты информации, в которых учтены наиболее распространённые компоненты автоматизированных систем обработки данных, например, представленные на рисунке 2.

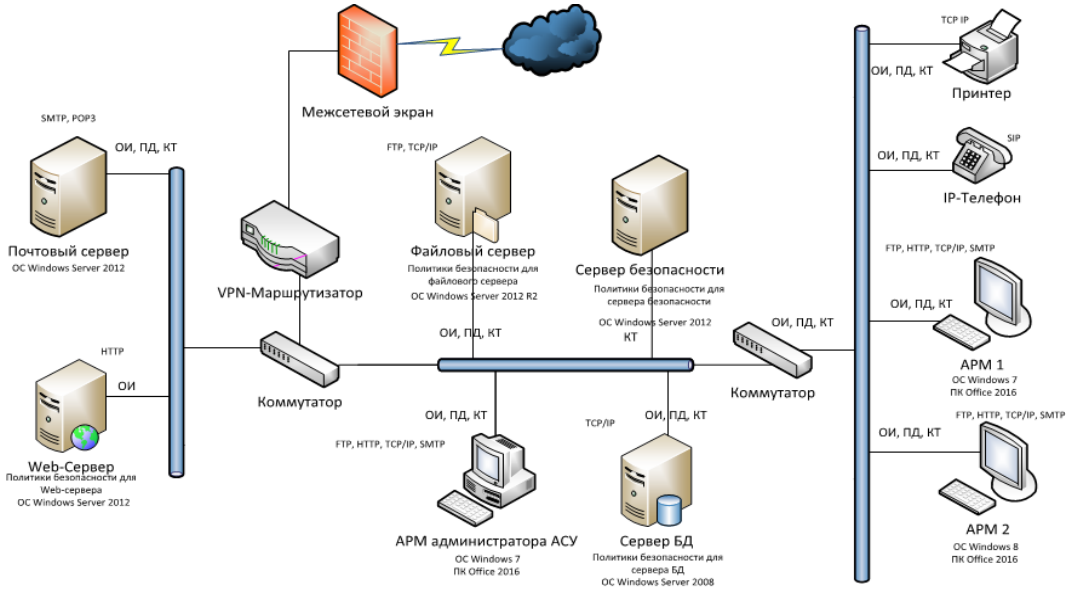

Рисунок 2-Пример типовой СЗИ защиты данных в организации
Figure2- Example of a typical data protection system in an organization

Параметры защитных мер предлагается закодировать по схеме в соответствии с Рисунком 3. Для этого необходимо предварительно определиться с порядком нумерации настроек.

№	h																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	0	1	0	1	0	0	0	5	0	0	0	0	0	0	5	4	0	5	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0	2	0	0	0	0	0	0	4	0	0	6	4	0	0	0	0	0
3	1	0	0	0	0	0	0	5	0	4	0	0	0	0	5	0	0	4	0	4	0	0	0	0	0
4	Режим подключения к сети со статической трансляцией адресов на ViPNet Coordinator HW 1000																								
5	Идентификация и аутентификация пользователей в программном комплексе ЗИ от НСД «Страж NT»																								
6	Контроль подключения съёмных носителей информации в программном комплексе ЗИ от НСД «Страж NT»																								
7	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	4	0	0	0	0	0

Рисунок 3-Пример конфигурации СЗИ
Figure 3-Sample configuration of Information Security System

Числа в представленной кодировке интерпретируются так:

- если *i*-я настройка в *j*-ой конфигурации не активирована или недоступна, *i*-я компонента вектора h_j равна 0;
- если *i*-я настройка включена в *j*-ой конфигурации, то *i*-я компонента вектора h_j равна некоторому числу, с помощью которого закодирован номер СЗ (или сочетания СЗ), где эта настройка установлена.

Например, пусть используются СЗ (межсетевой экран различных производителей и т.д.) с имеющейся настройкой (защита от DDoS-атак). Тогда возможные варианты настройки СЗ могут быть связаны с цифровым кодом так:

- настройка отключена -1;
- настройка включена на межсетевом экране ViPNet Coordinator HW 1000 -2;
- настройка включена на SecretNet Studio -3;
- настройка включена на межсетевом экране DallasLock 8.0-K-4.

Для описания связей между множеством настроек и множеством средств, а также связей между настройками и средствами защиты будем использовать матрицы сравнения.

Например, пусть задана матрица:

$A = ||a_{ij}||$, где a_{ij}- значение, отражающее совместимость (несочетаемость, конфликт) пары СЗ или настроек в них,$i = \overline{1,n}$, $j = \overline{1,n}$.

Значения a_{ij}могут быть не только бинарными. Но можно для описания связей между настройками задавать матрицы попарных сравнений (экспертно или на основе данных машинного обучения), где результаты сравнений определяются и иным способом, например:

$$a_{ij} = \begin{cases} 1, \text{если } i-\text{я настройка совместима с } j-\text{ой}, \\ 0, \text{если } i-\text{я настройка несовместима с } j-\text{ой}, \\ 0.3, \text{если } i-\text{я настройка плохо совместима с } j-\text{ой}, \\ \dots \end{cases}$$

Такое представление удобно и с учетом необходимости контроля настройки СЗ в соответствии с политиками ИБ и рекомендуемыми практиками, которые, как правило, содержат избыточное количество текста. Проще создать некоторый словарь терминов и обозначений для дальнейшего представления различных конфигураций в цифровом виде. Это облегчит их анализ и поиск оптимальных вариантов.

Вектора решений (конфигурации защиты) должны обладать одинаковыми размерностями для дальнейшей унификации входных данных и их обработки в процессе применения поисковых алгоритмов. К таким поисковым алгоритмам относится генетический алгоритм, использующий эволюционные аналогии при выборе наиболее адаптированных, “сильных” вариантов решений (в нашем случае, стратегий защиты).

Подходы к оценке эффективности конфигурации СЗИ с использованием имитационного моделирования

Эволюционные алгоритмы опираются на модель естественного отбора, сущность которого состоит в следующем: более приспособленные к внешним условиям биологические особи (в нашем случае – это варианты защиты, конфигурации СЗИ) имеют преимущество в выживании и размножении (устойчивости к атакам и сбоям). Хромосома в генетическом алгоритме будет ассоциироваться с определенным ранее вектором *h*.

Потомки более приспособленных особей также будут более сильными по сравнению с остальными. Для оценки приспособленности варианта решения необходимо задать функцию приспособленности. Защищенность системы, а, значит, и устойчивость к сбоям можно оценивать экспертным путем использования правил, заложенных, например, в основных нормативных документах. Так, методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» в соответствии с Таблицей 2, связывает меры защиты с классом защищенности, фактически - уровнем защищенности, эффективностью защищенности).

Для более объективной оценки эффективности конфигурации СЗИ можно учитывать не только сам факт наличия меры защиты, или рекомендуемых настроек на средствах защиты, но другие показатели, например, представленные в Таблице 3.

Таблица 2-Меры обеспечения доступности информации
Table 2 - Measures to ensure the availability of information

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ОДТ.3 (Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование)			+	+
Усиление ОДТ.3				1

Таблица 3- Показатели эффективности конфигурации СЗИ
Table 3- performance Indicators of the SPI configuration

Переменная	**Описание**
C	цена конфигурации СЗИ
V	весовой коэффициент важности защищаемых узлов (устройств), защищаемое СЗ
S	средний ущерб от простоя/утраты данных
T	время простоя при сбоях на устройстве
K	компетенция специалистов, поддерживающих работу СЗИ
P	вероятность успешности атаки /сбоя на защищаемый (-мом) узел(-ле)

Тогда функцию пригодности *F(h)* предлагается рассчитывать по формуле:

$$F(h) = C + \frac{V \cdot T \cdot S}{K} \cdot p \quad (1)$$

Затем задается некоторое эталонное значение функции пригодности $F_Б$ с допустимым отклонением β, учитываемым при оптимизационном поиске лучшего решения.

В формуле можно учесть:

- финансовую выгоду от нападения на определенные узлы сети организации (задание приоритетов),
- затраты, ресурсы, необходимые для разработки, модификации и внедрения сценария атаки,

- ущерб, включающий: ущерб от упущенной выгоды, штрафы за невыполнение условий договора по непрерывной работе информационных сервисов.

Не во всех случаях получается задать функцию пригодности, применимую для практического использования. Не все значения параметров в ней можно определить, измерить. Атаки на информационную систему зачастую носят случайный характер, т.е. невозможно заранее предугадать, какая из атак будет совершена в определенный момент времени и где.

Использование имитационной модели системы обуславливается еще и сложностями (занимает много времени, дорого, опасно) оценки эффективности используемых СЗИ на реальной (рабочей) системе. Можно оценить качество преодоления барьеров защиты на пути реализации атаки, используя при этом данные статистики и специализированных сайтов. В общем, термин «имитационное моделирование» означает, что если имеем дело с моделями, не позволяющими заранее вычислить или предсказать поведение системы, то для прогнозирования поведения системы необходим вычислительный эксперимент (имитация) на математической модели при заданных исходных данных [12-14].

Таким образом, будем считать, что система защиты представима в виде системы массового обслуживания (СМО), для которой определено множество угроз U_i.

СЗ подвергается некоторому набору сбоев ила атак A_i: перегрузка автоматизированного рабочего места (АРМ), перегрузка сервера (снижение производительности), критическая нагрузка на сервер (отказ в обслуживании), искажение информации на АРМ, отключение отдельного коммуникационного оборудования в КВИС (маршрутизатор, коммутатор).

Множество сбоев, атак характеризуется вектором интенсивностей $\lambda = \{\lambda_1, \lambda_1, \dots\}$, а подсистемы защиты S_i - различными характеристиками работы $\mu = \{\mu_1, \mu_1, \dots\}$. Каждой угрозе можно поставить в соответствие следующие параметры: частота возникновения угрозы; вероятность реализации угрозы; коэффициент разрушительности, выражающий степень разрушительности воздействия угрозы на актив(ы); набор активов или ресурсов, на которые направлена угроза и др. [15].

Возможно, осуществлять моделирование различных рубежей обороны на уровне сети, АРМ пользователя, операционной системы (ОС), системы управления базами данных и др.

В результате была разработана имитационная модель с использованием пакетов имитационного моделирования GPSS World, позволяющая оценить необходимые параметры системы при заданном векторе угроз и учете параметров окружающей среды. В имитационной модели было выбраны несколько категорий СЗИ: Межсетевой экран, Система обнаружения вторжений, Средство антивирусной защиты, а также различные активы, например сервера. Фрагмент модели:

```
Сегмент имитации выхода из строя OsnK
GENERATE ,,,1
Term1 ADVANCE (Exponential(12,0,T4)); Расчет времени до следующего отказа
FUNAVAIL OsnK; Выход из строя OsnK
SAVEVALUE Kont,1
ASSIGN 1,(Exponential(12,0,T7)); Расчет времени восстановления OsnK
ADVANCE P1 ; Имитация восстановления OsnK
SAVEVALUE VrOtk+,P1 ; Учет времени восстановления OsnK
```

FAVAIL OsnK ;OsnK в доступное состояние
TRANSFER ,Term1

Таким образом, возможным подходом при определении значений функции пригодности является использование имитационного моделирования, результаты которого оценивают параметры, участвующие в формуле (1).

Применение генетического алгоритма для поиска оптимальной конфигурации СЗИ

Полная процедура проведения исследования по подбору эффективной конфигурации СЗИ представлена на Рисунке 4.

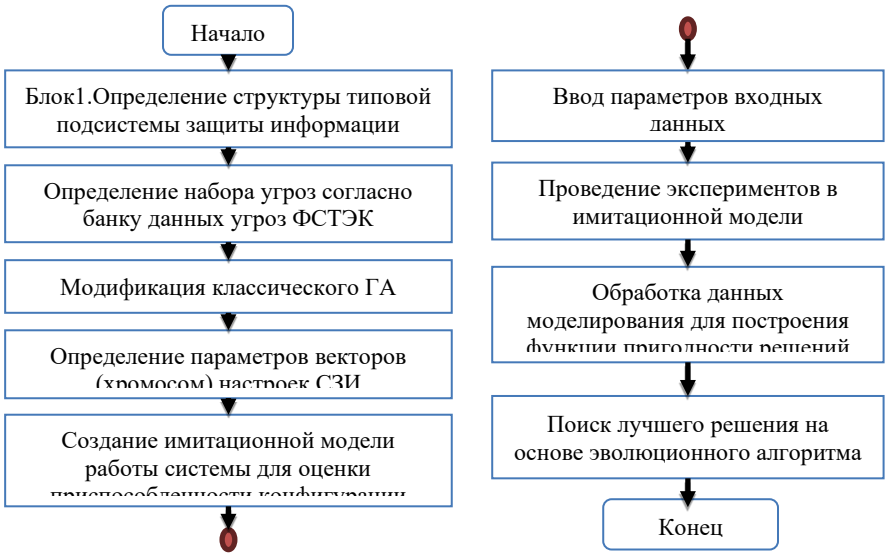

Рисунок 4-Процедура проведения исследования по подбору эффективной конфигурации СЗИ
Figure 4- Research procedure for selecting an effective configuration of the Information Security System

Классический генетический алгоритм включает различные операции над популяциями - селекция, скрещивание, мутация [16, 10]. В нашем случае модифицирован классический алгоритм в соответствии с блок-схемой, представленной на Рисунке 5.

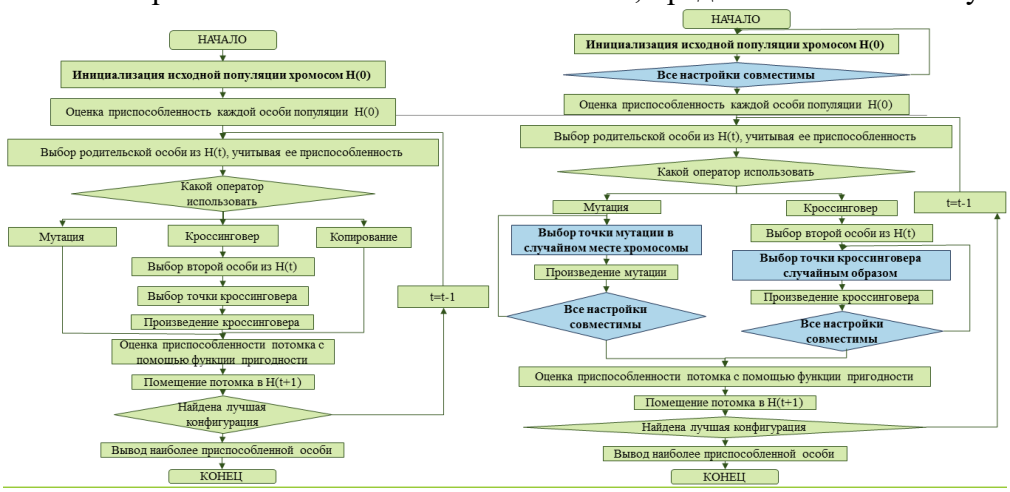

Рисунок 5-Блок-схема модифицированного генетического алгоритма поиска оптимальной конфигурации
Figure 5- Block diagram of the modified genetic algorithm for optimal configuration search

На этапе формирования исходной популяции происходит сравнение совместимости настроек в каждой хромосоме сгенерированной популяции по матрице совместимости настроек средств защиты. Операция мутации хромосом производится также при учете матрицы совместимости настроек средств защиты в случайном месте хромосомы.

При одноточечном кроссинговере выбирается одна точка разрыва внутри хромосомы, в которой две родительские хромосомы делятся на две части и обмениваются ими. При скрещивании невозможно производить “разрез” родительских хромосом в произвольном месте, так как это может привести к тому, что новое решение содержит недопустимые настройки СЗ. Все указанные ограничения были учтены в расчетах.

Заключение

Современные существующие на рынке средства защиты информации являются дорогостоящими и не решают такие, проблемы, как:

- неопределенность условий функционирования информационной системы, поведения системы защиты в нестандартных и экстремальных ситуациях;
- необходимость пересмотра концепции и программы информационной защиты, а впоследствии корректировки или замены текущих моделей СЗИ в связи с быстрым развитием информационных технологий;
- возможность обнаружения и прогнозирования атак, использующих технологии искусственного интеллекта.

Преимущества предложенного подхода - автоматизация решения повседневных задач специалистов по безопасности, решение вопроса нехватки квалифицированных кадров.

В ходе работы был проведен анализ применения эволюционных алгоритмов в информационной безопасности. Изучена структура и принципы работы эвристических алгоритмов оптимизации, модифицирован и адаптирован классический генетический алгоритм под решения задачи выбора эффективной конфигурации СЗИ.

ЛИТЕРАТУРА

1. ФСТЭК про оценку эффективности ИБ. Доступно по адресу: https://bis-expert.ru/blog/2560/49379 (дата обращения 19.05.2020)
2. Оценка качества СЗИ на основе анализа профиля безопасности. Доступно по: адресу https://studwood.ru/1615883/informatika/otsenka_kachestva_osnove_analiza_profilya_bezopasnosti (дата обращения 19.05.2020)
3. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014. Доступно по адресу: https://www.garant.ru/products/ipo/prime/doc/70567284/ (дата обращения 19.05.2020)
4. Оценка защиты информации. Доступно по адресу: https://spravochnick.ru/informacionnaya_bezopasnost/ocenka_zaschity_informacii/ (дата обращения 25.09.2019)
5. Приказ ФСТЭК РФ от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Доступно по адресу: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения 19.05.2020)

6. Актуальные киберугрозы I квартал 2019 года. Доступно по адресу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/ (дата обращения 19.05.2020)
7. CheckPoint на максимум. Человеческий фактор в информационной безопасности Доступно по адресу: https://habr.com/ru/company/tssolution/blog/334052/ (дата обращения 19.05.2020)
8. Шрейдер М.Ю., Боровский А.С., Тарасов А.Д. Проектирование систем физической зашиты с помощью генетического алгоритма. Вестник евразийской науки. 2017;4(41).Доступно по адресу: https://cyberleninka.ru/article/n/proektirovanie-sistem-fizicheskoy-zaschity-s-pomoschyu-geneticheskogo-algoritma. (дата обращения 19.05.2020)
9. Давидюк Н.В. Разработка системы поддержки принятия решений для обеспечения физической безопасности объектов. Дисс.канд.техн.наук. Астрахань, Изд.-во АГТУ, 2010.
10. Давидюк Н.В., Белов С.В. Процедура эффективного размещения средств обнаружения на объекте защиты с использованием метода генетического поиска. Информация и безопасность. 2009;12(4):559-568
11. Власов А.О. Формирование базы решающих правил системы обнаружения атак с помощью генетического алгоритма. Безопасность информационного пространства: материалы XII Всероссийской науч.-практ. Конф. студентов, аспирантов и молодых ученых. Екатеринбург. 2014:126-133
12. Киселев Д.Ю., Киселев Ю.В., Бибиков В.В. Имитационное моделирование информационных систем в пакете Arena. Самара: Изд-во СГАУ, 2014, 20 с.
13. Курилов Ф.М. Моделирование систем защиты информации. Приложение теории графов. Технические науки: теория и практика: материалы III Междунар. науч. Конф. Чита. 2016:6-9.
14. Сайт компании-разработчика системы имитационного моделирования AnyLogic. Доступно по адресу: http://www.anylogic.ru (дата обращения 20.05.2020)
15. Банк данных угроз безопасности информации ФСТЭК России. Доступно по адресу: https://bdu.fstec.ru/vul/2018-00979 (дата обращения 20.05.2020)
16. Давидюк Н.В., Белов С.В. Формирование начальной популяции в процедуре генетического поиска варианта эффективного расположения средств обнаружения на объекте защиты. Вестник Астраханского государственного технического университета. Серия: управление, вычислительная техника и информатика.2010;1:114-118.

REFERENCES

1. FSTEK pro otsenku effektivnosti IB (FSTEC about the assessment of the effectiveness of information security) Dostupno po adresu: https://bis-expert.ru/blog/2560/49379 (In Russ) (data obrashcheniya 19.05.2020 g.).
2. Otsenka kachestva SZI na osnove analiza profilia bezopasnosti (Evaluation of the quality of information security tools based on the analysis of the security profile) Dostupno po adresu:https://studwood.ru/1615883/informatika/otsenka_kachestva_osnove_analiza_profilya_bezopasnosti (In Russ) (data obrashcheniya 19.05.2020 g.).
3. Metodika otsenki sootvetstviia informatsionnoi bezopasnosti organizatsii bankovskoi sistemy Rossiiskoi Federatsii trebovaniiam STO BR IBBS-1.0-2014 (Methodology for assessing the compliance of information security of organizations of the banking system of the Russian Federation with the requirements of STO BR IBBS-1.0-2014) Dostupno po

adresu: https://www.garant.ru/products/ipo/prime/doc/70567284/ (In Russ) (data obrashcheniya 19.05.2020 g.).
4. Otsenka zashchity informatsii (Assessment of information security) Dostupno po adresu: https://spravochnick.ru/informacionnaya_bezopasnost/ocenka_zaschity_informacii/ (In Russ) (data obrashcheniya 19.05.2020 g).
5. Prikaz FSTEK RF ot 11 fevralia 2013 g. N 17 «Ob utverzhdenii trebovanii o zashchit einformatsii, ne sostavliaiushchei gosudarstvennuiu tainu, soderzhashcheisia v gosudarstvennykh informatsionnykh sistemakh».) Dostupno po adresu: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (In Russ) (data obrashcheniya 19.05.2020 g.).
6. Aktual'nye kiberugrozy I kvartal 2019 goda. Dostupno po adresu: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/ (In Russ) (data obrashcheniya 19.05.2020 g.).
7. Check Point na maksimum. Chelovecheskii faktor v informatsionnoi bezopasnosti. Dostupno po adresu: https://habr.com/ru/company/tssolution/blog/334052/ (In Russ) (data obrashcheniya 19.05.2020 g.).
8. Shreider M.Iu., Borovskii A.S., Tarasov A.D. Design of physical protection systems using a genetic algorithm. Vestnik evraziiskoi nauki. 2017;4(41). Dostupno po adresu:: https://cyberleninka.ru/article/n/proektirovanie-sistem-fizicheskoy-zaschity-s-pomoschyu-geneticheskogo-algoritma (In Russ) (data obrashcheniya 19.05.2020 g.).
9. Davidiuk N.V. Development of a decision support system to ensure the physical security of facilities. Cand.tech.sci. diss. Astrakhan, ASTU Publ., 2010.In Russ)
10. Davidiuk N.V., Belov S.V. Protsedura effektivnogo razmeshcheniia sredstv obnaruzheniia na ob"ektezashchity s ispol'zovaniem metoda geneticheskogo poiska [The procedure for the effective placement of detection tools at the facility using the genetic search method]. Informatsiiai bezopasnost' - Information and Security. 2009;12(4):559-568(In Russ)
11. Vlasov A.O. Formirovanie baz yreshajushhih pravil systemy obnaruzhenij aatak s pomoshh'ju geneticheskogo algoritma.Bezopasnost' informacionnogo prostranstva: materialy XII Vserossijskoj nauchno-prakticheskoj. konferencii studentov, aspirantov I molodyh uchenyh [Information Space Security: Materials of the XII All-Russian Scientific and Practical Conference of Students, Postgraduates and Young Scientists]. Ekaterinburg. 2014: 126-133.(In Russ)
12. Kiselev D.Ju., Kiselev Ju.V., Bibikov V.V. Imitacionnoe modelirovanie informacionnyh sistem v pakete Arena. Samara, 2014.In Russ)
13. Kurilov F.M. Modelirovanie system zashchity informatsii. Prilozhenie teorii grafov [Modeling of information security systems. Application of graph theory]. Tekhnicheskienauki: teoriiaipraktika: materialy III Mezhdunar. nauch. konf. [Technical Sciences: theory and practice: proceedings of the III International scientific conference]. Chita.2016:6-9(In Russ)
14. Sait kompanii-razrabotchika sistemy imitatsionnogo modelirovaniia AnyLogic. Dostupno po adresu: http://www.anylogic.ru (In Russ) (data obrashcheniya 20.05.2020 g.).
15. Bank dannykh ugroz bezopasnosti informatsii FSTEK Rossii. Dostupno po adresu: https://bdu.fstec.ru/vul/2018-00979 (In Russ) (data obrashcheniya 20.05.2020 g)
16. Davidiuk N.V., Belov S.V. Formation of the initial population in the genetic search procedure for the option of effective location of the detection means at the object of protection. Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: upravlenie, vychislitel'naia tekhnika I informatika - Bulletin of the Astrakhan State

Technical University. Series: control, computer engineering and informatics. 2010;1:114-118. (In Russ)

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Космачева Ирина Михайловна, канд. техн. наук, доцент, кафедра Информационная безопасность, ФГОУ ВПО Астраханский Государственный Технический Университет, Институт информационных технологий и коммуникаций. Астрахань, Российская Федерация.
e-mail: ikosmacheva@mail.ru

Irina M. Kosmacheva, Phd, Associate Professor, Department Of Information Security, Federal State Budget Educational Institution Of Higher Education Astrakhan State Technical University, Astrakhan, Russian Federation.

Давидюк Надежда Валерьевна, канд. техн. наук, доцент, заведующая кафедрой Информационной безопасности, ФГОУ ВО Астраханский Государственный Технический Университет, Институт информационных технологий и коммуникаций. Астрахань, Российская Федерация.
e-mail: davidyuknv@bk.ru

Nadezhda V. Davidyuk, Head of the Department of Information Security, phD, Associate Professor, Department of Information Security, Federal State Budget Educational Institution of Higher Education Astrakhan State Technical University, Astrakhan, Russian Federation.

Сибикина Ирина Вячеславовна, канд. техн. наук, доцент, кафедра Информационная безопасность, ФГОУ ВПО Астраханский Государственный Технический Университет, Институт информационных технологий и коммуникаций. Астрахань, Российская Федерация.
e-mail: isibikina@bk.ru

Irina V. Sibikina, Phd, Associate Professor, Department Of Information Security, Federal State Budget Educational Institution Of Higher Education Astrakhan State Technical University, Astrakhan, Russian Federation.

Кучин Иван Юрьевич, канд. техн. наук, доцент, кафедра Информационная безопасность, ФГОУ ВПО Астраханский Государственный Технический Университет, Институт информационных технологий и коммуникаций. Астрахань, Российская Федерация.
e-mail: Kuchin@astu.org

Ivan Y. Kuchin, Phd, Associate Professor, Department Of Information Security, Federal State Budget Educational Institution Of Higher Education Astrakhan State Technical University, Astrakhan, Russian Federation.