DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.1.4

УДК 004.056
ББК 32.97

АЛГОРИТМ ОПТИМАЛЬНОГО ВЫБОРА АРХИТЕКТУРЫ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С УЧЕТОМ СПЕЦИФИКИ ОБЪЕКТА И ВЗАИМОДЕЙСТВИЯ МОДУЛЕЙ ЗАЩИТЫ

Таймураз Таймуразович Зангиев

Кандидат технических наук,
доцент кафедры компьютерных технологий и информационной безопасности,
Кубанский государственный технологический университет
tzang@mail.ru
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Елизар Саввич Тарасов

Кандидат технических наук,
доцент кафедры компьютерных технологий и информационной безопасности,
Кубанский государственный технологический университет
helisar@mail.ru
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Владимир Владимирович Сотников

Студент,
Кубанский государственный технологический университет
bubert9@gmail.com
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Залина Якубовна Тугушева

Студент,
Кубанский государственный технологический университет
zalina.tug@mail.ru
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Фатима Рашидовна Гунай

Студент,
Кубанский государственный технологический университет
gunay.1963@mail.ru
ул. Московская, 2, 350072 г. Краснодар, Российская Федерация

Аннотация. В статье приведены актуальные проблемы, связанные с учетом противоречивых требований при проектировании комплексных систем защиты информации (КСЗИ). Предложен подход к выбору и конфигурации средств КСЗИ, основанный на ролевой модели М. Белбина в интерпретации КСЗИ как команды, которая позволит выстроить целостный контур защиты информации. Продемонстрированы случаи проявления синергизма и эмерджентности, обеспечивающие эффективное функционирование системы.

Ключевые слова: ролевая модель, синергия, эмерджентность, контур защиты.

При использовании информационных технологий все большее внимание уделяется аспектам информационной безопасности (ИБ), что обусловлено растущим из года в год ущербом, наносимым в результате инцидентов ИБ.

В результате увеличения этого ущерба наблюдается количественный и качественный рост рынка программных и аппаратных средств обеспечения информационной безопасности. При этом разрабатываются как новые альтернативы уже существующим средствам обеспечения ИБ, так и средства защиты от новых векторов атак, связанных, например, с распространением технологий концепции «Интернета вещей», больших данных и облачных технологий.

Вместе с тем анализ инцидентов информационной безопасности на предприятиях, активно использующих средства защиты информации, показал, что использование СЗИ не обеспечивает требуемый уровень эффективности защиты объектов информатизации, которые остаются подверженными атакам. Согласно недавно проведенным исследованиям, доля корпоративных систем на территории РФ, содержащих критически опасные уязвимости, связанные с неправильным конфигурированием СЗИ, составила более 80 %. При этом затраты российских компаний на обеспечение информационной безопасности увеличиваются в среднем на 30 % в год [2].

Одной из причин подобного явления является отсутствие системного подхода при выборе мер реализации комплексной системы защиты информационных объектов.

Заслуживают внимания подходы к построению концепций, моделей и алгоритмов системы защиты информационных объектов, когда основные идеи подсказаны самой природой. Как правило, внимательное наблюдение за окружением приводит к результатам с неожиданными эффектами, при этом одинаково полезно обращать внимание на поведение всего сущего в мире людей, животных, насекомых на макро- и микроуровнях.

Сегодня в системах защиты удачно используются как знания генетических алгоритмов, так и особенности моделей, построенных на основе принципов функционирования иммунных систем [3].

При проектировании целостного контура защиты объекта информатизации, как правило, используются несколько модулей системы защиты информации.

В этом случае полезно вспомнить работу группы людей, объединенных решением одной задачи или достижением одной цели [1].

Исследования показали, что эффективные команды имеют в своем составе членов, способных выполнять определенные роли. Мередит Белбин приводит восемь основных командных ролей, которые определяются личностными характеристиками членов команды, и описывает их типичные черты, положительные качества и допустимые недостатки. Число полезных ролей ограничено, и успех команды зависит от сочетания ролей и от того, насколько хорошо эти роли выполняются.

Важность каждой командной роли доказана опытом работы команд, в которых отдельные роли оставались вакантными. В работе команд с вакансиями всегда можно увидеть недостатки, связанные с неполным набором ролей. Успех командной работы зависит от сбалансированности состава команды. Предполагается наличие командных игроков с достоинствами, компенсирующими недостатки коллег. В этом случае слабости отдельных членов команды не будут мешать проявлению их сильных сторон.

Если представляется возможность создать сбалансированную команду, то предпо-

лагается, что члены команды будут подобраны на основе тестирования. При тестировании определяется способность потенциального члена команды выполнять каждую из восьми ролей с различными уровнями эффективности: низкой, средней, высокой и очень высокой.

Оптимально в команду следует включать лиц, имеющих «очень высокую способность» к выполнению роли, и при этом набор этих ролей должен быть полным. Роль, получившая оценку «высокая», рассматривается как резервная роль, к выполнению которой респондент может перейти, если выполнение первой роли не востребовано. Роли с оценками «низкая» и «средняя» указывают на слабые стороны респондента, и ему не рекомендовано пытаться выполнять эти роли, так как работа команды в целом будет иметь низкое качество.

Так как каждый член команды может выполнять несколько ролей, то число членов команды может быть меньше восьми. Исследования показывают, что число членов команды может быть от трех до двенадцати. Оптимальное число членов 5–8 человек. При увеличении размера команда рискует стать менее эффективной и может подвергнуться разделению; при уменьшении размера появляется риск невыполнения поставленных задач.

Таким образом, в сбалансированной команде проявляется эффект синергии, позволяющий увеличить производительность и существенно повысить способность команды к решению сложных творческих и инновационных задач.

Поэтому при построении контура защиты и выборе модулей системы защиты информации следует учитывать взаимодействие не только модулей с объектом защиты, но и взаимодействие этих модулей между собой. Формально модули систем защиты информации представимы в виде следующих классов, реализующих соответствующую функциональность:

– Антивирусы (защита в реальном времени, устранение уязвимостей, восстановление системы и файлов после атаки, регулярность обновлений);

– Межсетевые экраны (пакетная фильтрация, фильтрация на основе проверки содержимого, защита в реальном времени, гибкость использования);

– Средства контроля и разграничения доступа, в том числе средства идентификации и аутентификации (ИАФ) (надежность ИАФ, реализация правил разграничения доступа субъектов и их процессов, SIEM-функционал, предотвращение утечки данных, ограничение программной среды);

– VPN (быстродействие, безопасность, гибкость, конфиденциальность);

– Системы обнаружения и предотвращения вторжений (защита в реальном времени, обнаружение попыток нарушения безопасности, выявление аномалий в действиях пользователя, выявление аномалий во внешнем сетевом окружении, способность устранения уязвимостей);

– Средства защиты информации (от копирования/изменения/удаления) (обеспечение целостности, быстродействие, гибкость использования, отказоустойчивость, надежность удаления);

– Системы анализа защищенности (эффективность анализа, регулярность обновлений, анализ в реальном времени, способность устранения уязвимостей);

– Средства защиты среды виртуализации (контроль доступа виртуальной среды, управление виртуальными машинами и потоками информации, SIEM, обеспечение целостности).

При этом величину уровня достижения требуемой функциональности модулей возможно измерить путем экспертной оценки и факторного анализа, особенно в случае сложных, территориально распределенных систем. В качестве примера рассмотрим два программных продукта, реализующих функции антивируса (AV) и системы обнаружения и предотвращения вторжений (IPS) (см. рис. 1, 2).

В процессе проектирования системы защиты информации решаются две разнохарактерные задачи. Первой задачей является соблюдение минимальных требований к функционалу СЗИ, обусловленных как нормативно-правовыми документами (к примеру, приказами № 17 и 21 ФСТЭК России), так и, к примеру, внутренними корпоративными стандартами, максимально рациональным образом, то есть с минимизацией финансовых затрат (см. рис. 3). Второй задачей является достижение максимальных

показателей защищенности ИС в рамках выделенного бюджета.

В случае использования экспертной оценки функциональности средств защиты информации необходимо аналогичным образом оценивать требования, предъявляемые к системе защиты в целом.

Рассматривая проектируемый контур защиты как систему, можно прийти к выводу о возможности синергизма используемых модулей системы защиты информации. Действительно, если рассмотреть функционал защитного контура, реализованного на базе модулей СЗИ, продемонстрированных на рисунках 1 и 2, можно увидеть, что часть приведенных на рисунках функционалов аддитивна между собой.

Легко видеть, что использование двух средств защиты в составе контура делает возможным достижение заданного уровня функционалов, обеспечить который СЗИ поодиночке не в состоянии (см. рис. 4).

Представленные в статье требования к защитному контуру носят исключительно наглядный характер. В действительности к системе защиты информации предъявляется целый комплекс разнородных требований. При эффективном использовании предложенного

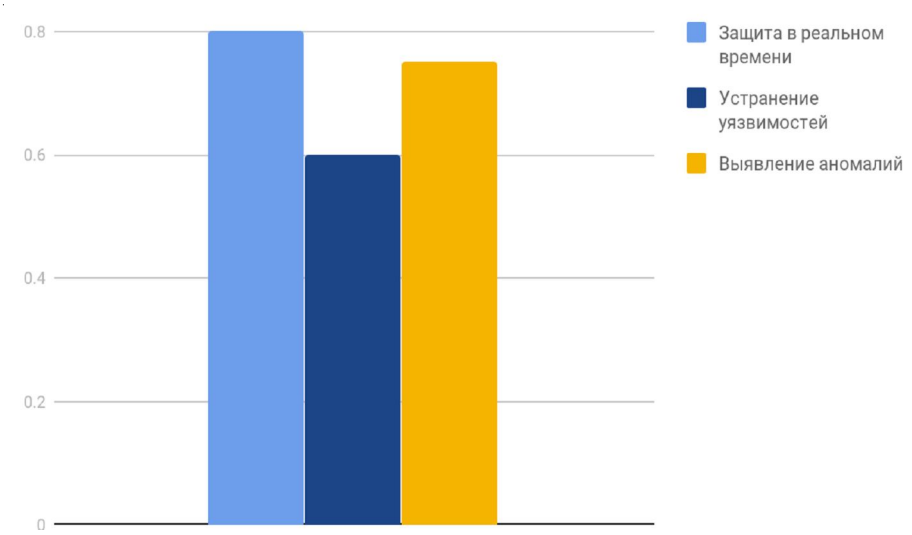

Рис. 1. Уровень функциональности IPS

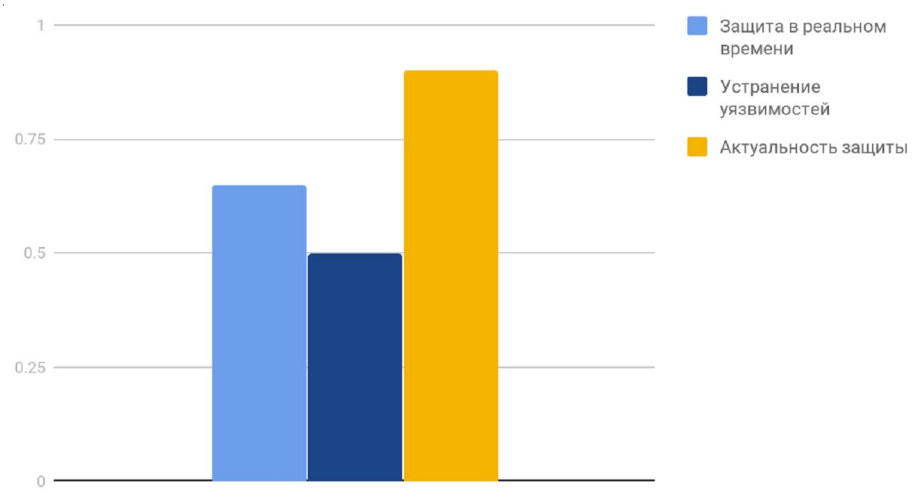

Рис. 2. Уровень функциональности AV

подхода выполнение данных требований возможно выполнить максимально рационально.

При этом следует учитывать, что в случае применения подобного подхода к системам со сложной информационной инфраструктурой взаимодействие СЗИ может иметь нетривиальный характер, требующий дальнейшего исследования. В частности, выражения для оценки уровня итоговой функциональности может быть представлено в виде комбинации функций, чаще всего – нелинейных. Более того, при детальном анализе функциональности тех или иных модулей СЗИ можно обнаружить у них наличие функций ряда других модулей. К примеру, межсетевой экран может также выполнять функции антивирусного продукта. Данная особенность позволяет добиться обеспечения требуемого уровня защиты меньшим числом модулей и, как следствие, с меньшими финансовыми затратами, что, в свою очередь, позволяет с большей эффективностью выполнить задачу максимизации показателей защищенности ИС в рамках ограниченного бюджета.

В некоторых случаях компоненты защитного контура могут проявлять свойства эмерджентности. Примерами подобного являются сценарии совместного применения средств МСЭ и VPN, когда МСЭ начинает выполнять функции увеличения надежности VPN, исключая возможность передачи интранет-трафика в обход VPN-сервера. Более распространенной практикой обеспечения защиты информации, использующей свойства эмерджентности ком-

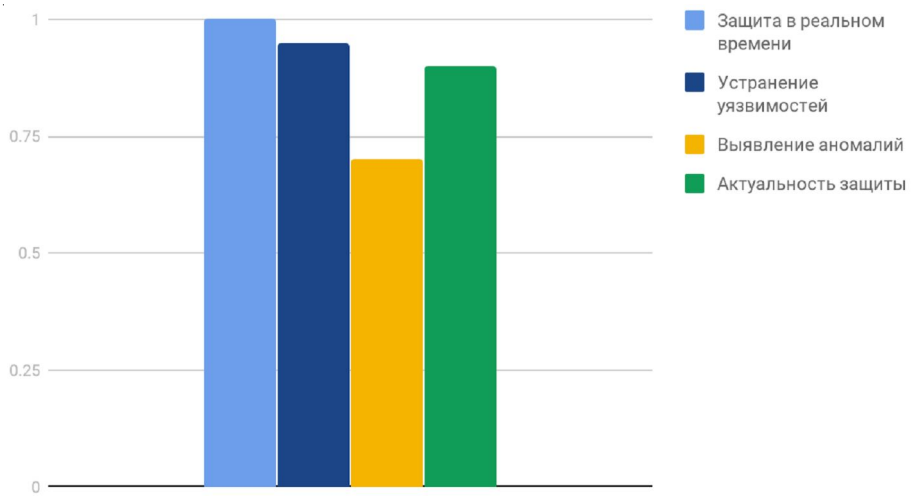

Рис. 3. Требуемый уровень функциональности модулей СЗИ

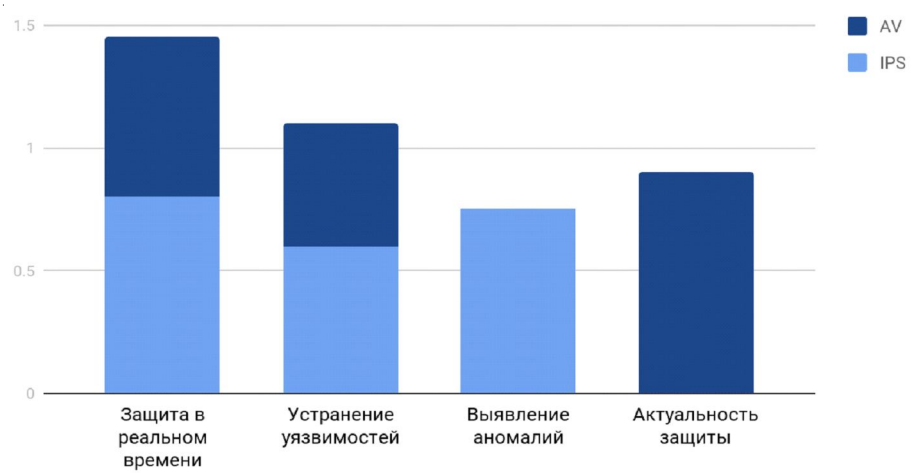

Рис. 4. Итоговый уровень функциональности контура СЗИ

понентов защитного контура, является использование компонентов МСЭ и АВЗ.

Таким образом, представленный подход к выбору и сочетанию компонентов архитектуры КСЗИ с учетом планируемого синергетического эффекта за счет взаимодействия модулей позволит достичь требуемого уровня функциональности разрабатываемой системы при существенном сокращении издержек.

Отметим также значительное увеличение эффективности КСЗИ в целом за счет явления эмерджентности, возникающей в результате использования ролевой модели при формировании требований к архитектуре.

СПИСОК ЛИТЕРАТУРЫ

1. Белбин, Р. Мередит. Команды менеджеров. Секреты успеха и причины неудач : пер. с англ. / Р. Мередит Белбин. – М. : HIPPO, 2003. – 315 с.

2. Статистика уязвимостей корпоративных информационных систем. – Электрон. дан. – Positive Technologies, 2016. – Режим доступа: URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Corporate-Vulnerability-2016-rus.pdf. – Загл. с экрана.

3. Частикова, В. А. Методика обнаружения полиморфных вирусов на основе искусственных иммунных систем и генетических алгоритмов / В. А. Частикова, М. Ю. Березов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2016. – № 124. – С. 744–755.

REFERENCES

1. Meredit Belbin R. *Komandy menedzherov. Sekrety uspekha i prichiny neudach* [Team of Managers. The Secrets of Success and the Causes for Failure]. Moscow, HIPPO Publ., 2003. 315 p.

2. Statistika uyazvimostey korporativnykh informatsionnykh sistem [Statistics of the Vulnerabilities of Corporate Information Systems]. *Positive Technologies*, 2016. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Corporate-Vulnerability-2016-rus.pdf.

3. Chastikova V.A., Berezov M.Yu. Metodika obnaruzheniya polimorfnykh virusov na osnove iskusstvennykh immunnykh sistem i geneticheskikh algoritmov [The Method of Detecting Polymorphic Viruses Based on Artificial Immune Systems and Genetic Algorithms]. *Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta*, 2016, no. 124, pp. 744-755.

ABOUT ONE APPROACH TO THE SELECTION OF INFORMATION PROTECTION FACILITIES

Taimuraz Taimurazovich Zangiev

Candidate of Sciences (Engineering),
Associate Professor, Department of Computer Technologies and Information Security,
Kuban State Technological University
tzang@mail.ru
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Elizar Savvich Tarasov

Candidate of Sciences (Engineering),
Associate Professor, Department of Computer Technologies and Information Security,
Kuban State Technological University
helisar@mail.ru
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Vladimir Vladimirovich Sotnikov

Student,
Kuban State Technological University
bubert9@gmail.com
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Zalina Yakubovna Tugusheva

Student,
Kuban State Technological University
zalina.tug@mail.ru
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Fatima Rashidovna Gunay

Student,
Kuban State Technological University
gunay.1963@mail.ru
Moskovskaya St., 2, 350072 Krasnodar, Russian Federation

Abstract. Much attention in the sphere of information technology is paid to the aspects of information security, due to the growing damage. As a result of damage increase, there is a quantitative and qualitative growth in the market of software and hardware for information security. At the same time, new alternatives to existing information security tools are being developed, as well as means of protection against new vectors of attacks associated, for example, with the spread of the concept of 'Internet of things', big data and cloud technologies.

At the same time, the analysis of information security incidents at enterprises that actively use information security tools shows that the use of information security systems does not provide the required level of protection for information objects that remain susceptible to attacks. According to recent studies, the share of corporate systems in the Russian Federation containing critical vulnerabilities associated with incorrect configuration of information security systems makes up more than 80 %. At the same time, the costs of Russian companies to ensure information security are increasing by an average of 30 % per year.

The article presents current problems related to the conflicting requirements to the design of complex information security systems (CISS). The authors suggest an approach to selection and configuration of the CISS facilities based on the role model of M. Belbin in the interpretation of the CISS as a command that will allow building an integrated information protection circuit. The cases of manifestation of synergism and emergence, which ensure the effective functioning of the system, have been described.

Key words: role model, synergy, emergence, protection circuit.