Scientific and Practical Cyber Security Journal (SPCSJ) 1(1):10-19

Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

BUILDING CYBER-SECURITY SYSTEMS OF INFORMATION NETWORKS BASED ON INTELLECTUAL TECHNOLOGIES

S. Toliupa, V. Nakonechny, N. Brailovskyi

Taras Shevchenko National University of Kyiv

ABSTRACT

Information technology has a significant impact on the level of technological and social development, economic competitiveness and safety of individual organizations, industries, departments, as well as the state as a whole. However, these technologies have a number of vulnerabilities due to the high interest of malicious elements in obtaining various benefits from this type of action. The level of a network's security is a consequence of the effectiveness of compatible methods and data protection means. To achieve these goals, there are many different approaches, techniques and analysis techniques. Special methods of secure coding and management of IP traffic are developed and used. However, as the studies have shown, a number of significant disadvantages prevent the efficient use of modern data protection tools in full.
The purpose of the article is to develop information protection management in the segment of the local information system to solve the problems of providing the required level of information security from cyber-excerpts in the course of the life cycle of the information security system in the conditions of uncertainty of information influences with the use of intellectual decision support.

KEYWORDS: cybersecurity, cyber threats, cyberattack, information technology, cyberspace, model, decision support system, protection.

АННОТАЦИЯ:

Информационные технологии оказывают существенное влияние на уровень технологического и социального развития, экономической конкурентоспособности и безопасности отдельных организаций, отраслей, ведомств, а также государства в целом. Однако, данные технологии имеют ряд уязвимостей, обусловленных высокой заинтересованностью злоумышленных элементов в получении различной выгоды от подобного рода действий. Уровень обеспечения сетевой безопасности является следствием эффективности соответствующих методов и средств защиты данных. Для достижения данных целей существует множество различных подходов, методик и технологий анализа. Разрабатываются и используются специальные методы безопасного кодирования и управления трафиком информационной системы. Однако, как показали исследования, ряд существенных недостатков не позволяет эффективно использовать современные средства защиты данных в полном объеме.
Целью статьи является разработка управления кибербезопасностью в сегменте локальной информационной системы для решения задач обеспечения требуемого уровня защищенности информации от кибервторжений в течение жизненного цикла системы защиты информации в условиях неопределенности информационных воздействий с использованием интеллектуальной поддержки принятия решений.

На современном этапе развития информационных технологий (ИТ) обеспечения кибербезопасности (КБ) в масштабах всей информационной системы пока еще затруднительно в силу отсутствия на рынке реальных решений, позволяющих строить именно интегрированные системы безопасности. Это можно объяснить недостаточной зрелостью международных

стандартов в области КБ, хотя движение з этом направлении прослеживается уже достаточно явно. С другой стороны построение многокомпонентных, а тем более однокомпонентных систем защиты информации (СЗИ) в большинстве случаев уже не является современным решением проблемы КБ, особенно для крупных компаний. Поэтому, на наш взгляд, в настоящее время оптимальным решением является построение именно комплексных систем кибербезопасности построенных на основе использования интеллектуальных технологий [1].

В последнее время все большей опасностью является хакерские кибератаки, проведенные с помощью вредоносного программного обеспечения. Именно этот вид компьютерной преступности в 2014-2017 годах достиг максимальной популярности и используется для реализации различных угроз кибербезопасности. Уровень обеспечения сетевой безопасности является следствием эффективности соответствующих методов и средств защиты данных. Для достижения данных целей существует множество различных подходов (сигнатурный, эвристический), методик (статическая, динамическая и др.) и технологий (стационарные, облачные и др.) анализа. Разрабатываются и используются специальные методы безопасного кодирования и управления трафиком ИС. Однако, как показали исследования, ряд существенных недостатков не позволяет эффективно использовать современные средства защиты данных в полном объеме. Возникает противоречие между расширением спектра злоумышленного программного обеспечения, повышением уровня киберпреступности в ИС, существующим состоянием основных технологий сетевой защиты и жесткими требованиями к информационной безопасности [2].

Успешное использования современных информационных технологий необходимо эффективно управлять не только сетью, но и СЗИ, при этом на уровне ИС автономно должна работать система, реализующая управление составом событий информационной кибербезопасности, планирование модульного состава СЗИ и аудит. Поскольку объект управления – СЗИ является весьма сложной организационно-технической системой, функционирующей в условиях неопределенности, противоречивости и неполноты знаний о состоянии киберпространства, управление такой системой должно быть основано на применении системного анализа, методов теории принятия решений и необходимой интеллектуальной поддержки [3].

Таким образом, целью статьи является разработка систем управления защитой информации в сегменте локальной информационной системы для решения научно-практической задачи обеспечения требуемого уровня защищенности информации в течение жизненного цикла системы защиты информации в условиях неопределенности информационных воздействий с использованием интеллектуальной поддержки принятия решений.

Проведенный анализ существующих стандартов в области менеджмента информационной безопасности позволяет сделать вывод о том, что целью стандартов является формирование общих понятий и этапов управления. Вместе с тем, стандарты не формируют конкретных подходов к управлению безопасностью, они определяют функциональные требования в отношении средств защиты й не предлагают методик сравнительного анализа различных комплексов средств защиты в целях выявления наиболее рационального варианта СЗИ.

Для реализации упреждающей стратегии защиты в СЗИ сегмента локальной информационной системы возникает необходимость разработки практически применимых моделей и методов интеллектуальной поддержки планирования рационального модульного состава СЗИ, оценки и прогнозирования риска нарушения информационной безопасности и управления защитой информации в условиях неопределенности информационных воздействий.

Главным направлением поиска путей защиты информации является неуклонное повышение системности подхода к самой проблеме кибербезопасности. Понятие системности интерпретировалось прежде всего в том смысле, что кибербезопасность заключается не только в создании соответствующих механизмов, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла систем обработки данных при комплексном использовании всех имеющихся средств киберзащиты. При этом все средства, методы и мероприятия, используемые для защиты информации, непременно и наиболее рационально объединяются в единый целостный механизм - систему кибербезопасности [4-5].

Основные трудности реализации систем защиты от киберугроз состоят в том, что они должны удовлетворять двум группам противоречивых требований. С одной стороны, должна быть обеспечена надежная защита находящейся в системе информации, что в более конкретном выражении формулируется в виде двух обобщенных задач: исключение случайной и преднамеренной выдачи информации посторонним лицам и разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала. С другой стороны, системы защиты не должны создавать заметных неудобств в процессе работы с использованием ресурсов системы. В частности должны быть гарантированы: полная свобода доступа каждого пользователя и независимость его работы в пределах предоставленных ему прав и полномочий. К сожалению, необходимость системного подхода к вопросам обеспечения безопасности информационных технологий пока еще не находит должного понимания у пользователей современных ИС.

Основываясь на принципах системного анализа, который представляет собой теорию и практику улучшающего вмешательства в проблемную ситуацию, предлагается вариант декомпозиции проблемы разрешения имеющихся противоречий в области обеспечения безопасности информации.

На основании системного подхода показано, что модель проблемной ситуации в области защиты информации содержит совокупность трех взаимодействующих систем: СЗИ, которая имеет проблемные вопросы в безопасности, системы управления принятия решения информационной безопасностью, которая разрабатывается для того, чтобы проблема исчезла или ослабла, окружающей среды, с которой взаимодействует СЗИ, под которой понимается множество потенциально возможных киберугроз информационной безопасности. Требование постоянно нарастающей детализации приводит к построению модели состава проблемосодержащей системы, модели объекта защиты и модели киберугроз [6].

Следует отметить, что основной проблемой при построении управляющей системы является разработка модели киберугроз, что связано со специфичностью взаимодействия объекта управления – СЗИ с окружающей средой. В связи с этим предлагается концепция построения модели киберугроз безопасности информации, базирующаяся на разрабатываемой классификационной схеме преднамеренных целенаправленных киберугроз информационной среде локальной информационной системы. Показывается целесообразность построения совокупности моделей: функциональной, на основе описания последовательности действий злоумышленника (нарушителя) с помощью деревьев угроз, и пространственной графовой, систематизированных в формате интегральной структурной модели каналов несанкционированного доступа, утечки и деструктивных воздействий, позволяющей провести всесторонний анализ реальных киберугроз, повысить адекватность модели угроз для конкретного объекта защиты.

На основе анализа принципов управления в условиях неопределенности предлагается обобщенная структура системы управления защитой информации в сегменте локальной информационной системы (рис. 1), которая включает две функциональные подсистемы: подсистему

организационно-технического управления и подсистему оперативного управления в реальном масштабе времени.

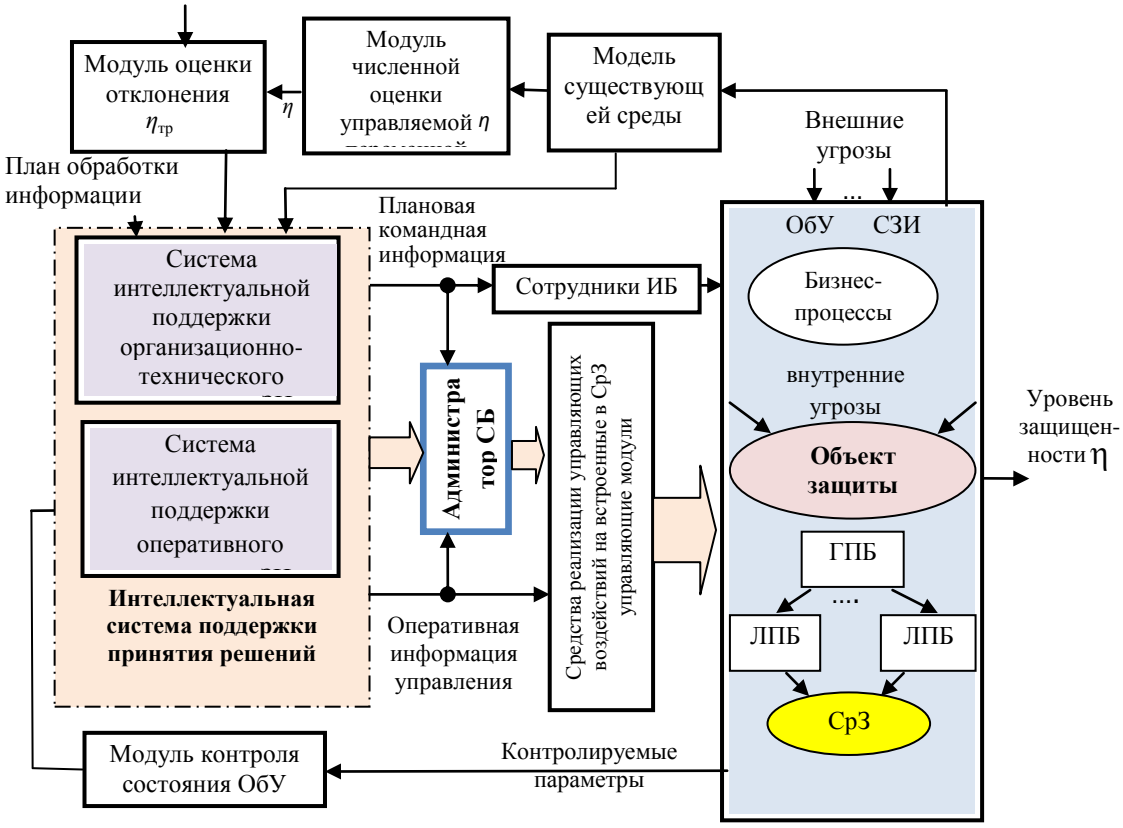

Рисунок 1 – Обобщенная структура системы управления защитой информации в сегменте локальной информационной системы, которая включает две функциональные подсистемы: подсистему организационно-технического управления и подсистему оперативного управления в реальном масштабе времени: ОбУ (СЗИ) – объект управления; ГПБ, ЛПБ – глобальная, локальные политики безопасности; СрЗ – средства защиты; $\eta_{тр}$ – требуемое значение уровня защищенности

В контуре организационно-технического управления создаются механизмы управления защитой информации при изменении инфраструктуры, бизнес-приложений, планов обработки информации и соответствующих им требований к уровню защищенности информации. Контур включает: систему интеллектуальной поддержки принятия решений по выбору стратегии защиты, систему оценки уровня защищенности (риска), управляющее воздействие реализуется сотрудниками отдела информационной безопасности. Командная информация формируется в ходе планирования – целенаправленного выбора рационального комплекса средств защиты.

В контуре оперативного управления формируется оперативная командная информация, которая доводится до объекта управления администратором безопасности или автоматически с помощью средств реализации управляющих воздействий на встроенные в средства защиты управляющие модули.

В системе управления, имеющей такое архитектурное построение, эффективные решения выбираются и принимаются как на основе сведений о технических характеристиках средств защиты, так и на основе анализа контролируемого киберпространства.

На основе анализа возможностей совершенствования управления защитой информации за счет применения новых методов решения задач управления и сокращения длительности цикла управления разрабатывается функциональная модель системы управления в позволяющая наглядно и эффективно отобразить механизм управления ЗИ, выявить процессы, для реализации которых необходима разработка автоматизированной системы интеллектуальной поддержки управления.

На основе теоретико-множественного подхода предлагается формализованное описание информационной системы, созданной в соответствии с рекомендуемыми международными стандартами основными принципами архитектуры безопасности, с помощью модели, отображающей семантику предметной области. Предлагается описание множества атак в виде кортежей

$$U^{\text{внш}} = \langle S^{\text{внш}}, \text{А}, \text{З}_\text{с}, \text{З}_\text{х}, \text{П}, O(C) \rangle \tag{1}$$

$$U^{\text{вн}}_{l(m)} = \langle S_l^{k-1}, \text{А}, \text{З}_\text{с}, \text{З}_\text{х}, \text{П}, O^k(C_m^k) \rangle,$$

где $U^{\text{внш}}$ – удаленная кибератака на информационные активы сегмента информационной системы; $U^{\text{вн}}_{l(m)}$ – внутренняя кибератака на информационные активы уровня критичности *k*, обрабатываемые в сегментах С_m, когда нарушитель имеет учетную запись как пользователь с правом доступа к информации, уровень критичности которой не более (*k*-1), и пытается превысить свои привилегии; $S^{\text{внш}}$ – внешний источник киберугрозы; S_l^{k-1} – внутренний источник киберугрозы; А – коммуникационное оборудование в канале связи; $\text{З}_\text{с}, \text{З}_\text{х}$ - сервисы безопасности на пути распространения кибератаки, сетевые и хостовые; П – протоколы, пакеты; *O* – объект доступа; C_m^k – сегмент, в котором обрабатывается информация, наивысший уровень критичности которой равен *k*; *l, m*– номера сегментов.

Приводится оценка числа путей распространения кибератак, анализируется возможность идентификации кибератаки по индикаторам аномальных событий на пути распространения. С помощью характеристического предиката вводится множество индикаторов

$$И = \{u_j : u_j - \text{индикатор сетевой, хостовый или периметров ый}\}. \tag{2}$$

Поскольку единственным эффективным способом идентифицировать кибератаку является анализ комбинаций аномальных событий, предлагается сопоставлять множеству возможных путей *P* распространения кибератак множество индикаторов

$$\tau_a \subseteq P \times \text{И} = \{(p_i, \text{и}_j) : p_i \in P \ \wedge \ \text{и}_j \in \text{И}\}, \tag{3}$$

а вероятность того, что подозрительная активность является кибератакой, оценивать числом индикаторов на пути распространения. Сечение соответствия по $\tau_a(p_i)$ определяет набор индикаторов, соответствующий реализации кибератаки на данном пути.

Так как в системе оперативного управления предъявляются требования к времени вычислений командной информации, то для решения задачи управления в условиях неполноты, противоречивости и неопределенности данных о состоянии киберпространства целесообразно использовать механизм нечеткого логического вывода. Информацией, которая поступает на вход системы нечеткого логического вывода, являются входные переменные – число признаков аномальных событий. Эти переменные соответствуют реальным процессам в сети. Информация, которая формируется на выходе системы нечеткого логического вывода, соответствует выходной переменной, которая является вероятностью того, что совокупность аномальных событий в сети является кибератакой (вероятность кибератаки).

Кроме такого похода выявления киберугроз, есть и другие, которые на основе анализа методов сетевых отказов (СО) (сигнатурный, статистический анализ, использование интеллектуальных систем, генетических алгоритмов, нейросетей), и на основании сравнительного анализа моделей СО позволяют сделать заключение о целесообразности применения комплексного подхода к решению задач противодействия киберугрозам и кибератакам, включающей статистические методы, в дополнении к сигнатурных систем, применяемых на практике, а как система, дающая возможность принять правильное решение, использовать интеллектуальную систему. Практика показывает, что у должностных лиц, от которых зависит качество и надежность функционирования системы безопасности, крайне мало времени на аналитическую работу, что позволяет избежать ошибок при принятии решений. Лучшим вариантом организации поддержки деятельности лиц, принимающих решения, является создание вокруг них среды человеко-машинной поддержки, в которой главная роль отводилась бы СППР [7-9].

Для реализации выбранного метода определения и идентификации КбА предлагаются модели сигнатурного и статистического анализаторов сетевого трафика, а для определения источников кибервторжений и выбора вариантов по их устранению - нечеткая интеллектуальная система.
При разработке интеллектуальной системы была выбрана нечеткая модель. Это связано с тем, что значительная часть информации о причинах и источники КбА может быть получена только экспертным путем или в виде эвристических описаний процессов. Для определения источников КбА система безопасности должна быть представлена моделью той информационной сети на которую она ориентируется.
Представим отдельный уровень системы безопасности в виде нелинейного объекта с множеством входных переменных и одной выходной переменной в $\{x_i\}, i = \overline{1,n}$:

$$y = f_y(x_1, x_2, \ldots, x_n) \quad (4)$$

Комплексная интеллектуальная система поддержки принятия решений (ИСППР) для определения вторжений содержит набор функциональных компонент, позволяющих максимально автоматизировать и ускорить выработку управляющих воздействий при изменении ситуации в системе безопасности. Структура информационной системы принятия решения для определения кибервторжений представлена на рис. 2.

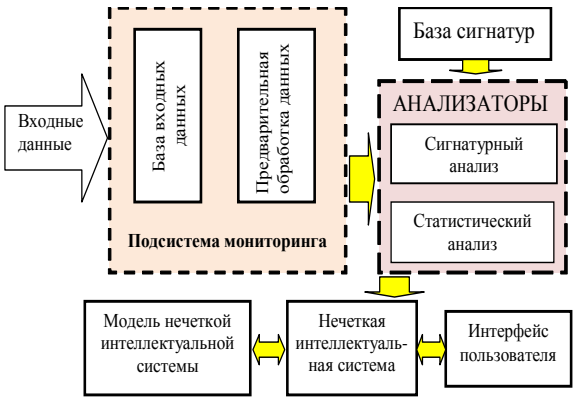

Рис. 2. Структура информационной поддержки принятия решеня при определении кибервторжений

Современный подход к построению систем обнаружения кибератак на информационные системы полон недостатков и уязвимостей, позволяющих, к сожалению, вредным воздействиям успешно преодолевать системы защиты информации. Переход от поиска сигнатур кибератак к выявлению предпосылок возникновения угроз информационной

безопасности должна способствовать тому, чтобы в корне изменить данную ситуацию, сократив дистанцию отставание в развитии систем защиты от систем их преодоления. Кроме того, такой переход должен способствовать повышению эффективности управления информационной безопасностью и, наконец, более конкретных примеров применения нормативных и руководящих документов.

В условиях, когда управляющая система не обладает полной информацией о состоянии информационной среды, обосновывается необходимость разработки модели противодействия киберугрозам, в которой существует возможность выбора того управляющего воздействия, которое в наибольшей степени соответствует состоянию объекта управления. Формулируются принципы разработки модели противодействия киберугрозам, приводится формализованное описание метода принятия решений по выбору рационального варианта реагирования на события безопасности.

Процесс выбора рационального варианта реагирования на события безопасности описывается кортежем

$$\langle U_i, V_j, C(V_j), P_{\text{a}}, P(z_l), J, U*(P_{\text{a}})\rangle, \tag{5}$$

где U_i – вариант реагирования; V_j – исход; C_j – оценка ущерба; z – параметр неопределенности состояния среды; $P(z_l)$ – вероятность состояния среды; J – целевая функция выбора; $U^*(P_{\text{a}})$ – рациональный вариант реагирования; P_{a} – вероятность кибератаки.

Анализ возможных вариантов реагирования $\{U_i\}$ на события безопасности показал, что число управляющих воздействий для каждой ситуации ограничено, $i \in [1,3]$. Поскольку выбор осуществляется в условиях возможного осуществления кибератаки, предлагается связывать систему предпочтений альтернатив с оценкой ущерба: отсутствие ущерба, ущерб одному пользователю, ущерб группе пользователей, ущерб от реализации кибератаки ($\{V_j\}, j \in [1,4]$).

Задается функционал, по которому осуществляется выбор рационального варианта реагирования:

$$J(U_i, z) = \sum_{l=1}^{s} C_j\left(V_j(U_i, z_l)\right) \cdot p(z_l), \tag{6}$$

где $p(z_l) = \prod_{i=1}^{I} p_{ij}\left(V_j(U_i), P_{\text{a}}\right)$, вероятности p_{ij} наступления каждого *j*-го исхода при выборе *i*-го варианта реагирования предлагается рассчитывать как функции вероятности кибератак

$$p_{ij} = p_{ij}\left(V_j(U_i), P_{\text{a}}\right), \qquad \forall i : \sum_j p_{ij} = 1. \tag{7}$$

Рациональное управляющее воздействие $U^*(P_{\text{a}})$ определяется как

$$U^*(P_{\text{a}}) = U\left(\arg\min_i\left(J(U_i, z)\right)\right). \tag{8}$$

На основе адаптированного для выбора рационального варианта реагирования метода принятия решений разрабатываются модели противодействия киберугрозам с учетом возможных путей их распространения: локальное сетевое вторжение, по радиоканалу через беспроводную точку доступа, удаленное вторжение через сети открытого доступа.

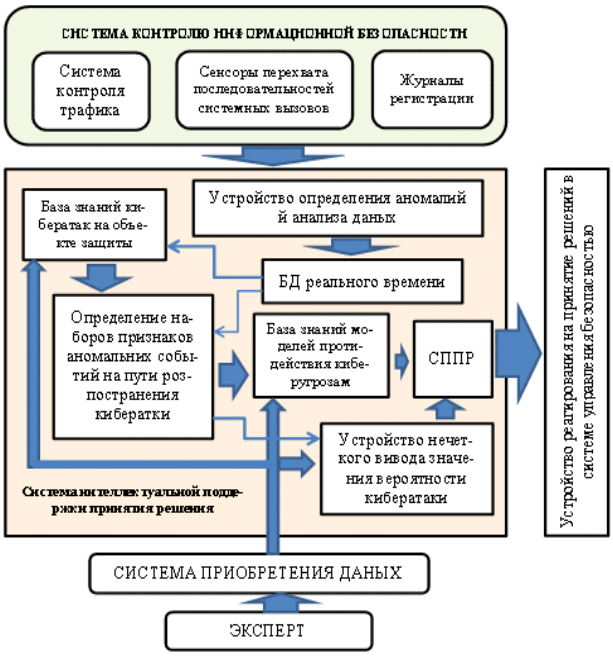

Рис. 3 - Структура системы интеллектуальной поддержки управления системой кибербезопасности

Для преодоления трудностей в слабоформализованных ситуациях более высокий качественный уровень управления в условиях реального времени предполагает обеспечение необходимой и достаточной интеллектуальной поддержки. Предлагаемая в работе структура построения системы интеллектуальной поддержки оперативного управления приведена на рисунке 3.

В системе интеллектуальной поддержки управления СБ предлагается использовать интеллектуальные технологии: механизм нечеткого логического вывода для численной оценки вероятности кибератаки; организованное упорядочение информации о событиях в базе знаний; модели противодействия угрозам; принятие решений по выбору рационального варианта реагирования на события безопасности.

Проблема разграничение системы защиты информации различной степени конфиденциальности заключается в том, что часто на практике в рамках одной ИС приходится «работать» с информацией, требования по защите, которой существенно отличаются друг от друга. Так обрабатываемые и хранимые в рамках типовой ИС информационные ресурсы, как правило, разделяются на три группы: открытые информационные ресурсы, конфиденциальные информационные ресурсы, информационные ресурсы ограниченного доступа,

Очевидно, что защита всех разновидностей информационных ресурсов в рамках одной и той же СБ подразумевает, что даже открытые ресурсы будут защищаться по требованиям, предъявляемым к защите секретной информации. Очевидно, это приведет к необоснованно высокой стоимости СБ и большим неудобствам работы для персонала компании. Так же неэффективно будет построение трех различных СБ для каждого из ресурсов, поскольку, во-первых, четко разделить эти ресурсы в рамках одной ИС практически никогда не удается, а во-вторых, это опять приведет к повышению стоимости самой системы.

Для успешного использования современных информационных технологий необходимо эффективно управлять не только сетью, но и системой защиты информации этой сети. Система, реализующая управление составом событий информационной безопасности должна работать автономно, необходимо также разработать модель процесса планирования рационального модульного состава СБ каждого уровня, а также метод формирования рационального комплекса средств защиты на основе общих критериев [10].

В процессе управления в условиях реального времени, *планирование* СБ как функция управления представляет собой процесс последовательного *снятия неопределенности* относительно

структуры и *состава* средств защиты в СБ. Процесс планирования $P_{\text{пл}}$ рациональных наборов СрЗ характеризуется с помощью выражения

$$P_{\text{пл}} = \Phi \to S_r, \tag{9}$$

где Ф – множество функциональных подсистем для контура безопасности;

S_r– выбранный набор средств защиты.

На первом этапе задается множество функциональных подсистем для контура безопасности, результатом планирования является управляющая информация, которая содержит конкретные данные по распределяемым ресурсам, направляемым на достижение целевого состояния СБ.

Процесс принятия решения о выборе рационального варианта набора СрЗ для контура безопасности – это функция преобразования содержания информации о требованиях, предъявляемых к средствам защиты, входящим в набор, о характеристиках средств защиты, в подмножество наилучших вариантов набора $S' \subseteq S$. Множество вариантов набора

$$S = \{S_1, \text{K}, S_r, \text{K}, S_R\}, \tag{10}$$

где R – число вариантов альтернативных наборов, из которых осуществляется выбор.

Для выбора рационального варианта набора средств защиты используется целевая функция J:

$$S_r = J(S). \tag{11}$$

Совокупность сведений, позволяющих сопоставлять варианты наборов, это характеристики средств защиты функциональных подсистем для рубежа – множество W, включающее в себя два подмножества:

$$W_{\text{зщ}_l} \subset W_l \text{ и } W_{\text{и}_l} \subset W_l, \tag{12}$$

где $W_{\text{зщ}_l}$ – показатель средств защиты «защищенность информации»;

$W_{\text{и}_l}$ – показатель средств защиты «издержки» для l-ой функциональной подсистемы.

На основе морфологического подхода модель принятия решений по выбору рационального варианта набора может быть представлена в виде кортежа:

$$\text{ПР: } \langle \text{Ц}, \Phi, \Pi_s, S, W_l, J, S_r(S') \rangle, \tag{13}$$

где Ц – цель принятия решения;

Φ – исходные данные для порождения вариантов набора средств защиты:

$$\Phi = \{\Phi_1, \Phi_2, \text{K}, \Phi_l, \text{K}, \Phi_L\};$$

Π_s – правило порождения вариантов набора, которое может быть представлено в аналитическом виде как векторное произведение множеств

$$S = \Phi_1 \times \Phi_2 \times \text{K} \times \Phi_l \times \text{K} \times \Phi_L, \tag{14}$$

где Φ_l – множество, состоящее из средств защиты l-ой функциональной подсистемы

$$\Phi_l = \{A_{l1}, A_{l2}, \text{K}\ A_{lm}\ \text{K}, A_{lK_l}\}; \tag{15}$$

S– множество порожденных вариантов набора;

W_l – данные для выбора рациональных вариантов;

J – целевая функция для выбора рационального набора средств защиты(правило выбора);

S_r – рациональный набор средств защиты.

Отмечается, что в условиях автоматизированного управления и при использовании экспертной информации в процессе принятия решения можно говорить (даже в случае формализованного правила выбора) о *рациональном*, а не оптимальном решении.

Выводы. В соответствии с предлагаемой моделью защиты, основой планирования рационального модульного состава СБ являются функциональные требования к наборам СрЗ для каждого контура безопасности, которые формулируются на основе нормативной документации, в соответствии с уровнем критичности обрабатываемой информации. Альтернативные средства защиты для каждой функциональной подсистемы набора средств защиты выбираются с учетом этих требований. Вариантов наборов, сертифицированных по требуемому классу защищенности, может быть много. Сравнение вариантов наборов средств защиты предлагается производить по количественной мере. В системе интеллектуальной поддержки рациональные решения предлагается выбирать на основе использования экспертных знаний; в ней реализуется механизм приобретения знаний в процессе заполнения полей знаний экспертом при взаимодействии его с автоматизированной системой, выполняется совокупность процедур над проблемной областью с использованием многокритериального сравнительного анализа для выявления в заданном экспертом множестве подмножества наилучших по критериям предпочтения вариантов наборов, из которых формируется рациональный комплекс средств защиты.

ЛИТЕРАТУРА:

1. Толюпа С.В., Безрук В.М., Баранник В.В. и др. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, инфомационная боротьба. Коллективная монография. Харьков – Компания СМИТ – 2017. – с. 620.
2. Толюпа С.В., Успенский А.А. Построение систем захисту информации на основе многоуровневой иерархической модели.Information Technology and Security. July-December 2016. Vol. 4. Iss. 2 (7)
3. В.И. Андреев, Ю.Ю. Гончаренко, М.М. Дивизинюк, И.Н. Павлов, В.А. Хорошко. Проектирование систем технической защиты информации / - Севастополь.: Изд. Центр СНУЯЭиП, 2011. – 235 с.
4. Толюпа С.В., Пархоменко І.І. Побудова комплексних систем захисту складних інформаційних систем на основі структурного підходу. Науково-технічний журнал "Сучасний захист інформації".– 2015. - №4. – С. 96-104.
5. Толюпа С.В. Проектирование систем поддержки принятия решений в процессе восстановления и обеспечения комплексной защити информационных системах. // Науково-технічний журнал "Сучасний захист інформації".– 2012. - №4. – С. 69-74.
6. Бугайский К. В. Проблемы построения систем информационной безопасности // "Information Security/ Информационная безопасность". – М.: BHV, 2008. – 250 с.
7. Debar, H., Dacier, M., and Wespi, A. (1999), "Towards a Taxonomy of Intrusion Detection Systems," Computer Networks, vol. 31, 1999, pp. 805-22
8. Debar, H., Dacier, M., and Wespi, A. (2000), "A Revised Taxonomy for Intrusion-Detection Systems," presented at Annales des Télécommunications, vol. 55, 2000, pp. 361-78
9. Kabiri, P., and Ghorbani, A., A. (2005), "Research on Intrusion Detection and Response: A Survey", International Journal of Network Security, Vol.1, No.2, Sep. 2005, pp.84-102
10. Бабенко Л.К. Разработка комплексной системы обнаружения атак / Л.К. Бабенко, О.Б. Макаревич, О.Ю. Пескова // Информационная безопасность: материалы V междунар. науч. - практ. конф. 2003. №4(33). С.235 - 239