К ОРГАНИЗАЦИИ ИНТЕЛЛЕКТУАЛЬНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

НЕСТЕРУК Ф.Г.

УДК 681.5:002.5

Нестерук Ф.Г. **К организации интеллектуальной защиты информации.**
Аннотация. Рассмотрены вопросы организации системы защиты информации (СЗИ), структура которой ориентирована на процессы адаптации к динамике угроз и компьютерных атак. Показано, что в двухуровневой иерархической модели адаптивной СЗИ нижний адаптивный уровень, ответственный за оперативную реакцию на динамику внешнего окружения, должен быть интеллектуальным (по аналогии с иммунными механизмами биологической системы, которые работают автоматически, практически без коррекции со стороны центральной нервной системы), а верхний адаптивный уровень (соответствует процессам обобщения и запоминания центральной нервной системы) ориентирован на использование интеллекта администратора безопасности в качестве компонента модели.
Ключевые слова: защита информация, иерархическая модель адаптивной защиты, адаптация к угрозам, интеллектуальные средства защиты.

Nesteruk Ph.G. **To organization of intellectual protection of the information.**
Abstract. The systems of protection are considered which are adaptive to dynamics of threats and computer attacks. The two-level hierarchical model of adaptive protection is offered. The bottom adaptive level is intended for operative reaction to dynamics of an external environment. Therefore it should be intellectual (by analogy with immune mechanisms of biological system, which work automatically). The top adaptive level corresponds to processes of generalization and storing of the central nervous system. It is focused on use of intelligence of the safety manager as a component of model.
Keywords: protection the information, hierarchical model of adaptive protection, adaptation to threats, intellectual means of protection.

1. Введение. Своевременность предложенных на обсуждение материалов обусловлена тем, что системы защиты информации (СЗИ) должны быть сориентированы на оперативную реакцию при обеспечении безопасности информационно-коммуникационных систем (ИКС) в условиях высокой динамики угроз, изменения качественных и количественных характеристик компьютерных атак. Названная проблема может быть решена за счет применения интеллектуального подхода к разработке современных СЗИ [1, 2].

Производители программного обеспечения, например, Microsoft, заявляют о применении «технологии активной защиты» [3], основанной на оценке поведения программ с точки зрения их потенциальной опасности. СЗИ корректируют средства защиты ИКС при изменении статуса или блокируют работу, если возникает подозрение в заражении вирусом или проникновении злоумышленника [4].

Постановка задачи организации интеллектуальной защиты носит комплексный характер и использует биосистемную аналогию, начиная с формы представления информации, программирования информационных процессов и заканчивая архитектурой ИКС с встроенными механизмами обеспечения безопасности [2, 5].

Эволюция средств обработки информации осуществляется в направлении создания ИКС с элементами самоорганизации, в которых присутствуют процессы зарождения, приспособления и развития [6]. Эволюционные процессы лежат в основе жизнеспособности биологических систем, для которых характерны высокая защищенность, накопление опыта, селективный отбор.

Как известно [7, 8], биосистемы обладают многоуровневой иерархической системой жизнеобеспечения, реализованной с использованием комплекса механизмов информационной избыточности, защиты и иммунитета. Механизмы обеспечения безопасности современных ИКС по возможностям далеки от биологических прототипов, в связи с чем исследования в сфере организации интеллектуальной защиты, базирующиеся на биосистемной аналогии, представляются актуальными.

Статья посвящена обсуждению организации интеллектуальной защиты на базе модели двухуровневой иерархической СЗИ, использующей средства интеллектуального анализа информации.

Как известно информация – постоянно протекающий процесс субъект-объектного взаимодействия, а знание возникает и существует в процессе обмена информацией, т.е. в процессе формирования/корректировки логических связей (базы знаний – БЗ) между структурами данных (базой данных – БД) [9].

Рассмотрим принципы организации адаптивной СЗИ, ориентированные на биосистемную аналогию и динамику процессов взаимодействия потоков данных и структур [2, 9].

2. Модель адаптивной защиты ИКС. Модель адаптивной защиты ИКС – иерархическая многоуровневая модель, содержащая адаптивные средства классификации (АСК) на каждом из иерархических уровней СЗИ [10].

Связующим звеном модели адаптивной СЗИ является методика оценки защищенности ИКС, которая координирует взаимосвязь АСК угроз и АСК механизмов защиты (МЗ) в виде нейронных сетей (НС), нечетких НС, систем правил логического вывода, структурной модели системы информационной безопасности (СИБ), инструментальных средств расчета показателей защищенности и рейтинга ИКС (рис. 1). В

АСК могут быть использовать самоорганизующиеся НС, например, ARTMAP или EMANN [11-14].

Адаптивность позволяет при ограниченных затратах на организацию СЗИ обеспечить заданный уровень безопасности ИКС за счет оперативной реакции на изменение множества угроз. Не менее важным качеством является возможность фиксации в СЗИ *накопленного опыта* в виде информационных полей НС иерархии АСК.

Рис. 1. Модель адаптивной СЗИ.

В соответствии с заданием на проектирование СЗИ выбирается структурная модель СИБ в виде иерархии уровней механизмов защиты, а опыт экспертов представляется матрицами экспертных оценок (БД) и системами правил логического вывода (БЗ) для классификации угроз по признакам атак и МЗ на множестве известных угроз.

Системы правил логического вывода для последующей адаптации и анализа представляются в виде нечетких НС, которые обучают на некотором подмножестве входных векторов. Обучают также АСК в виде самоорганизующихся НС таким образом, чтобы число образуемых кластеров равнялось числу правил в БЗ.

Для матриц экспертных оценок производят расчет показателей и рейтинга защищенности ИКС [15], которые используются методикой оценки защищенности для оптимизации СЗИ, анализа и коррекции экспертных оценок, параметров АСК и правил логического вывода.

Информация в адаптивной СЗИ хранится и может наследоваться в виде распределенных адаптивных информационных полей НС: *поля известных угроз* иммунных уровней защиты и поля *жизненного опы-*

та рецепторных уровней защиты. Процесс адаптации информационных полей НС связан с решением задач классификации, кластеризации, приводящих к коррекции и расширению баз знаний.

Анализ пар «угроза-уязвимость» позволяет каждой угрозе, оговоренной в задании на проектирование СЗИ, – заданной угрозе из множества известных угроз, поставить в соответствие выявленные уязвимости ИКС. Если в качестве базовой модели выбрать многоуровневую систему информационной безопасности [16, 17], то модель адаптивной СЗИ, включающая минимальное число МЗ, достаточных для защиты выявленных уязвимостей ИКС, будет расширять множество механизмов защиты при выявлении новых угроз и уязвимостей [2, 18, 19].

Распределение МЗ по уровням иерархии модели СЗИ отражается на размерах матриц экспертных оценок, т.к. изменение в модели СЗИ приводит к появлению новой строки или столбца в матрицах оценок. Опыт экспертов представляется системой правил логического вывода, описывающих соответствие посылок и заключений. В рассматриваемой модели (рис. 1) нашли отражение иммунный (рис. 2) и рецепторный уровни СЗИ.

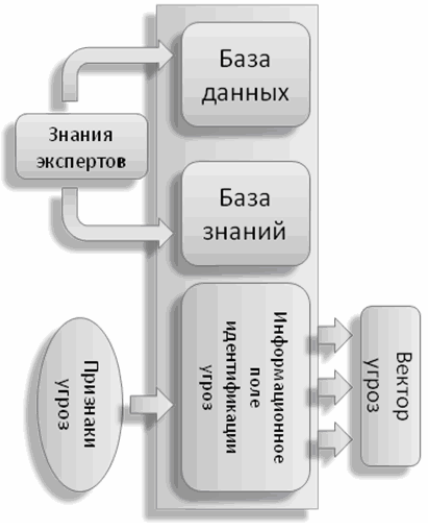

Рис. 2. Иммунный уровень адаптивной СЗИ.

Иммунный уровень решает задачу классификации угроз по признакам атак, а рецепторный решает сходную задачу классификации механизмов защиты по вектору угроз. Системы правил логического

вывода отображаются в топологии нечетких НС для последующего обучения и анализа результатов процесса адаптации.

АСК каждого из уровней СЗИ организованы по иерархической схеме: матрица экспертных оценок ↔ система правил логического вывода ↔ нечеткая НС ↔ самообучающаяся НС. Самообучающаяся НС необходима для решения задачи *кластеризации*. В процессе самообучения НС добиваются разбиения векторов обучающей выборки на группы, число которых равно числу правил в базе знаний. Решая задачу кластеризации, четкая НС для «нового» вектора посылок изменяет размерность вектора заключений, что вызывает добавление новых правил в БЗ и соответствующих нейронов в нечеткую НС. Обучение нечеткой НС и последующий анализ весов связей вновь введенных ФН позволяет сформировать спецификацию на отсутствующие в СЗИ механизмы защиты и откорректировать матрицу экспертных оценок.

В процессе работы СЗИ происходит *накопление опыта* эксплуатации ИКС за счет адаптации базы знаний, параметров нечетких НС, матриц экспертных оценок. Коррекция матриц экспертных оценок изменяет значения показателей защищенности ИКС, что позволяет отслеживать динамику защищенности и принимать решение о необходимости модификации СЗИ.

3. Модель интеллектуальной СЗИ. Знание – структурообразующее понятие, постоянный процесс изменения связей данных. Согласно [9] *информационная база* (ИБ) состоит из взаимосвязанных базы данных, базы знания и средств ее разработки и управления, а информационные процессы рассматриваются как субъект-объектное взаимодействие. Для организации субъект-объектного взаимодействия требуются две информационные базы, которые образуют *интеллектуальную базу* (рис. 3) [9]. Одна информационная база представляет жизненный опыт (“память”), а другая – “текущее состояние“ системы. Новые знания возникают в процессе взаимодействия информационных баз и стабилизации их структуры.

Рассмотрим, каким образом интеллектуальная база соотносится с моделью адаптивной СЗИ. Согласно модели [2, 10] система защиты ИКС может быть представлена двухуровневой иерархической структурой:

– нижний уровень – полностью автоматический за счет наличия интеллектуальной базы, которая самостоятельно набирает жизненный опыт в процессе «общения» через коммуникационную среду: одна информационная база представляет жизненный опыт (“память”), а другая - “текущее состояние“ СЗИ;

– верхний уровень ориентирован на получения информации о динамике изменения нижнего уровня и не является интеллектуальным и автоматическим, т.к. решение принимает администратор безопасности (он является интеллектуальной базой уровня). Однако уровень содержит базу знаний, базу данных и средства формирования/корректировки логических связей – БЗ между структурами данными – БД.

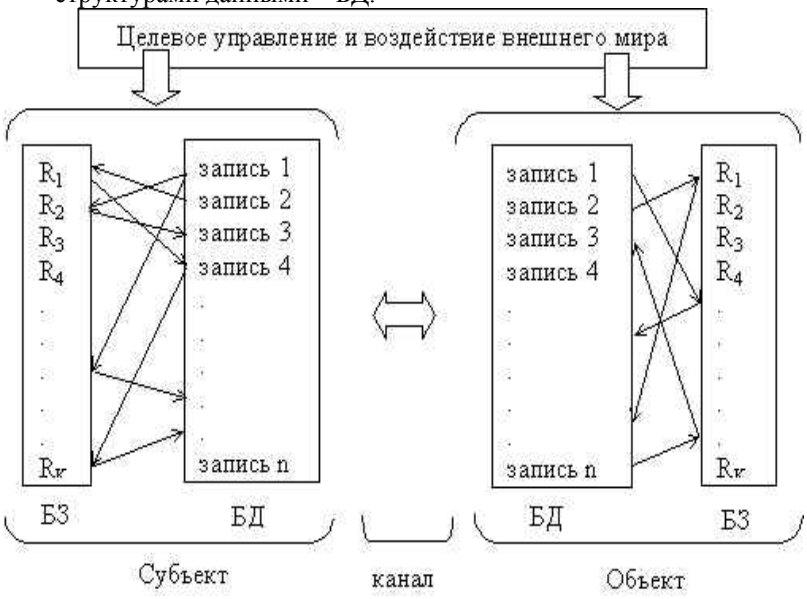

Рис. 3. К понятию интеллектуальной базы.

То есть при сохранении двухуровневой иерархии СЗИ, содержащей адаптивные средства классификации, назначение и функции уровней СЗИ разные:

– нижний становится интеллектуальным (аналог иммунных механизмов в организме, которые работают оперативно и автоматически, практически без коррекции со стороны головного мозга – центральной нервной системы организма);

– верхний соответствует процессам запоминания в центральной нервной системе организма, которая работает значительно медленнее и накапливает опыт под контролем и участии администратора безопасности.

Проиллюстрируем изменения в модели адаптивной СЗИ посредством рис. 4.

В момент создания интеллектуального уровня в него с верхнего уровня иерархии загружают (этап наследования – передачи опыта): исходные БД и БЗ, начальные методы их взаимодействия с внешним миром и их собственной коррекции.

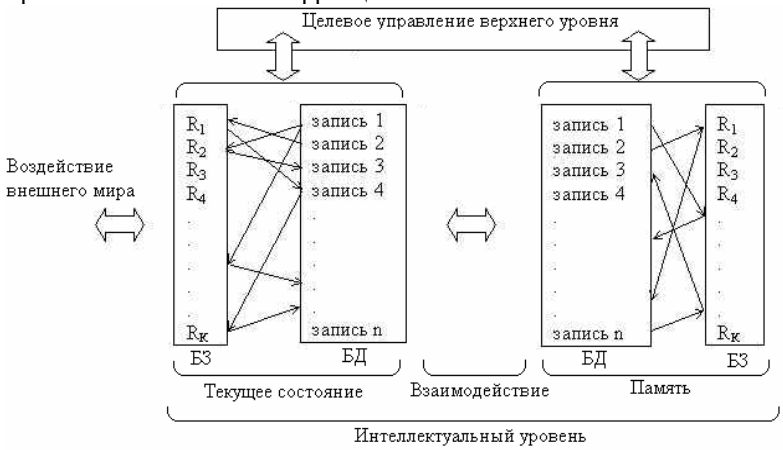

Рис. 4. Иерархия адаптивных уровней интеллектуальной СЗИ.

Нижний уровень постоянно взаимодействует с внешним миром (Интернетом, коммуникационной средой ИКС) и автоматически изменяется (постоянно реализуемый этап развития). Причем в процессе работы интеллектуального уровня в ИБ «Текущее состояние» изменяются как исходные БД и БЗ, так и методы их взаимодействия с внешним миром и их собственной коррекции (постоянно выполняемый этап развития – адаптация к внешним условиям, реализуется основное свойство – пластичности). А в ИБ «Память» также изменяются как исходные БД и БЗ, так и методы их взаимодействия с внешним миром и их собственной коррекции, но в результате взаимодействия с информационной базой «Текущее состояние» и целевых установок верхнего уровня (администратора безопасности) – фиксируются в памяти только существенные изменения, реализуется основное свойство – стабильности.

Верхний иерархический уровень СЗИ получает с нижнего уровня иерархии системы защиты динамику состояний как «памяти» (стабильность), так и «текущего состояния» (пластичность) с целью интеллектуального анализа (посредством АСК) и коррекции структурной модели СИБ (посредством методики оптимизации при участии *естественного интеллекта* администратора безопасности ИКС).

Для организации информационной связи с внешним миром необходимы посредники – параметры физической среды, через которые можно судить о динамике воздействия коммуникационной среды ИКС и Интернета. В качестве входных параметров может выступать:

- статистика ИКС (частота посещения ИКС, анализ сетевых адресов: из каких доменов, частота повторения адресов и пр.);
- статистика операционной системы (открытие, закрытие файлов, операции над файлами, временные параметры, попытки обращения к системным файлам и защищаемым областям памяти и пр.)

4. Заключение. В работе проиллюстрированы принципы организации интеллектуальной защиты ИКС, ориентированные на биосистемную аналогию и динамику процессов взаимодействия потоков данных и структур.

В качестве аппарата для исследования информационных процессов в сложных информационно-коммуникационных системах можно использовать теорию интеллектуального управления.

Представляется актуальной разработка адаптивных средств классификации в составе иерархической модели системы защиты информации или системы поддержки принятия решений, а также методик оптимизации их структуры путем отслеживания динамики внешнего окружения, моделирование процессов накопления опыта (формирования и коррекции знания) исходя из результатов интеллектуального анализа информации.

Адаптивный характер СЗИ связан с решением двух основных задач: задачи обеспечения автоматической и оперативной реакции системы защиты на изменение внешнего окружения, а также задачи формирования баз знаний, накопления опыта об изменении внешнего окружения и использования накопленных знаний для оптимизации размещения механизмов защиты на иерархических уровнях СЗИ.

Литература

1. *Нестерук Ф.Г., Молдовян А.А., Нестерук Л.Г., Нестерук Г.Ф.* Квазилогические нейронечеткие сети для решения задач классификации в системах защиты информации // Вопросы защиты информации. 2007, № 1. С. 23 – 31.
2. *Нестерук Ф.Г., Суханов А.В., Нестерук Л.Г. , Нестерук Г.Ф.* Адаптивные средства обеспечения безопасности информационных систем / Под ред. Л. Г. Осовецкого. – СПб.: Изд-во Политехнического университета, 2008. 626 с.
3. *Слива К.* Защита будет активной // Computerworld Россия. 2004, № 11. с. 49.
4. *Робертс* П. Защита на клиенте // Computerworld Россия. 2004, № 16. с. 44.
5. *Нестерук Г.Ф., Осовецкий Л.Г., Харченко А.Ф.* Информационная безопасность и интеллектуальные средства защиты информационных ресурсов. (Иммунология систем информационных технологий).– СПб.: Изд-во СПбГУЭФ, 2003. 364 с.

6. *Кузнецова В.Л., Раков М.А.* Самоорганизация в технических системах. – Киев: Наук. думка,1987.
7. *Лобашев М.Е.* Генетика. – Л.: Изд-во ленинградского университета, 1969. 679 с.
8. *Мелик-Гайказян И.В.* Информационные процессы и реальность. М.: Наука, 1998. 108 с.
9. *Лачинов В.М., Поляков А.О.* Информодинамика или Путь к Миру открытых систем. / Издание 2-е, перераб. и доп. – СПб.: Издательство СПбГТУ, 1999.
10. *Нестерук Г.Ф., Молдовян А.А., Нестерук Ф.Г., Костин А.А., Воскресенский С.И.* Организация иерархической защиты информации на основе интеллектуальных средств нейро-нечеткой классификации // Вопросы защиты информации, № 3, 2005. С. 16 – 26.
11. *Carpenter G.A., Grossberg S., & Reynolds J.H.* ARTMAP: Supervised Real-Time Learning and Classification of Nonstationary Data by a Self-Organizing Neural Network // Neural Networks, 4, 1991, P. 565 - 588.
12. *Granger E., Rubin M. A., Grossberg S., Lavoie P.* Classification of Incomplete Data Using the Fuzzy ARTMAP Neural Network // Proc. Int'l Joint Conference on Neural Networks, vol. IV, 2000, P. 35 - 40.
13. *Carpenter G.A., Grossberg S., Rosen D.B.* Fuzzy ART: Fast Stable Learning and Categorization of Analog Patterns by an Adaptive Resonance System // Neural Networks, 4, 1991, P. 759 - 771.
14. *Берсини Х.* Двойная пластичность иммунной сети. В кн. Искусственные иммунные системы и их применение / Под ред. Д. Дасгупты. Пер. с англ. под ред. А.А. Романюхи. — М.: ФИЗМАТЛИТ, 2006.
15. *Нестерук Ф.Г., Осовецкий Л.Г., Нестерук Г.Ф.* К оценке защищенности систем информационных технологий // Перспективные информационные технологии и интеллектуальные системы, № 1, 2004.
16. *Осовецкий Л., Шевченко В.* Оценка защищенности сетей и систем // Экспресс электроника. 2002. № 2-3. С.20-24.
17. *Мельников В.В.* Защита информации в компьютерных системах. - М.: Финансы и статистика; Электронинформ, 1997.
18. *Nesteruk Ph., Kharchenko A., Nesteruk G.* Information safety in electronic business: adaptive model of systems safety of information technologies // Proc. of the Int. Conf. "Information technology in business" (St. Petersburg, October 8-10, 2003) - St. Petersburg, 2003. P. 124-128.
19. *Нестерук Ф.Г., Нестерук Г.Ф., Харченко А.Ф.* Моделирование адаптивных процессов защиты информационных ресурсов экономических объектов // Сб. докл. междунар. НПК «Глобальные тенденции в статистике и математических методах в экономике». - СПб, 2004. С. 218-220.

Нестерук Филипп Геннадьевич — к.т.н.; старший научный сотрудник научно-исследовательского отдела проблем информационной безопасности (НИО ПИБ) Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: представление и обработка данных и знаний с неопределенностью, применение методов интеллектуального анализа информации в области информационной безопасности, технология разработки адаптивных систем защиты информации. Число научных публикаций — 32. 08p@mail.ru; СПИИРАН, 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178, РФ; р.т. +7(964)-333-33-14. Научный консультант — А.А. Молдовян.

Nesteruk Philip Genad'evich — PhD in CS; senior researcher, Research Department of Safety Problems, St. Petersburg Institute for Informatics and Automation of the Russian Acad-

emy of Sciences (SPIIRAS). Research interests: uncertain knowledge and data representation and processing, intellectual analysis methods in information safety, technologies and development of adaptive systems of safety. The number of publications — 32. 08p@mail.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; phone +7(964)-333-33-14. The scientific adviser — A.A.Moldovyan

Рекомендовано научно-исследовательским отделом проблем информационной безопасности, заведующий отделом Молдовян А.А., д. т. н., проф.
Статья поступила в редакцию 10.12.2009.

РЕФЕРАТ

Нестерук Ф.Г. **К организации интеллектуальной защиты информации.**

Рассмотрены принципы организации адаптивных систем защиты информации (СЗИ) на базе средств интеллектуального анализа информации. Обсуждается двухуровневая иерархия СЗИ на базе средств интеллектуального анализа информации:

- нижний уровень – полностью автоматический за счет наличия интеллектуальной базы, которая самостоятельно набирает жизненный опыт в процессе «общения» через коммуникационную среду Интернета: одна информационная база представляет жизненный опыт (“память”), а другая - “текущее состояние“ СЗИ;

- верхний уровень ориентирован на получения информации о динамике изменения нижнего уровня и не является интеллектуальным и автоматическим, т.к. решение принимает администратор безопасности (он является интеллектуальной базой уровня). Однако уровень содержит базу знаний, базу данных и средства формирования/корректировки логических связей (БЗ) между структурами данными (БД).

То есть при сохранении двухуровневой иерархии СЗИ, содержащей адаптивные средства классификации, назначение и функции уровней СЗИ разные:

- нижний становится интеллектуальным (аналог иммунных механизмов в организме, которые работают оперативно и автоматически. Практически без коррекции со стороны головного мозга – центральной нервной системы организма);

- верхний соответствует процессам запоминания в центральной нервной системе организма, которая работает значительно медленнее и накапливает опыт под контролем и участии администратора безопасности.

В момент создания интеллектуального уровня в него с верхнего уровня иерархии загружают (этап наследования – передачи опыта): исходные БД и БЗ, начальные методы их взаимодействия с внешним миром и их собственной коррекции.

Нижний уровень постоянно взаимодействует с внешним миром (Интернетом) и автоматически изменяется (постоянно реализуемый этап развития). Причем в процессе работы интеллектуального уровня в ИБ «Текущее состояние» изменяются как исходные БД и БЗ, так и методы их взаимодействия с внешним миром и их собственной коррекции (постоянно выполняемый этап развития – адаптация к внешним условиям, реализуется основное свойство – пластичности). А в ИБ «Память» также изменяются как исходные БД и БЗ, так и методы их взаимодействия с внешним миром и их собственной коррекции, но в результате взаимодействия с информационной базой «Текущее состояние» и целевых установок верхнего уровня (администратора безопасности) – фиксируются в памяти только существенные изменения, реализуется основное свойство – стабильности.

SUMMARY

Nesteruk Ph.G. **To organization of intellectual protection of the information.**

The adaptive systems of defence are considered on the base of intellectual facilities. The two-tier hierarchy of the system of defence comes into question on the base of intellectual facilities:

- a lower level of hierarchy is automatic because there is an intellectual base which accumulates experience of exploitation in the process of «intercourse» through an of communication environment: one informative base presents experience of exploitation ("memory"), and other is "current status" of the system of defence;

- the top level of hierarchy gets information about the dynamics of lower level and is not intellectual and automatic, because the administrator of safety makes decision (he is the intellectual base of level). A level contains the knowledges base – KB, database – DB and forming mean / adjustments of logical connections (KB) between structures information (DB).

That setting and functions of levels of defence changes in the two-tier hierarchy of the system of defence:

- the lower level of hierarchy becomes intellectual (analogue of immune mechanisms in an organism, which work operatively and automatically without a correction from the side of cerebrum - cns of organism);

- the top level of hierarchy corresponds to the processes of memorizing in the cns of organism, which works considerably slower and accumulates experience under control the administrator of safety.

At creation of intellectual level in him from the top level of hierarchy download (stage of inheritance and transmission of experience): initial DB and KB, initial methods of their co-operating with the outer world and their own correction.

A lower level co-operates with the outer world and changes automatically (permanent stage of development). Thus during work of adaptive level in an intellectual base «Current status» change both initial DB and KB and methods of their co-operating with the outer world and their own correction (adaptation to the external terms, property of plasticity). In an intellectual base «Memory» also change both initial DB and BZ and methods of their co-operating with the outer world and their own correction, but as a result of co-operating with an informative base «Current status» and by management signals top level (administrator of defence). Substantial changes are fixed in memory, and property of stability will be realized.