Bryukhomitsky Yuri Anatol'evich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: bya@tsure.ru; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; associate professor.

УДК 004.056.5 004.89

В.С. Аткина

МОНИТОРИНГ СОСТОЯНИЙ КАТАСТРОФОУСТОЙЧИВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ПОМОЩЬЮ ГИБРИДНОЙ ИММУННОЙ СЕТИ

Цель исследования: разработка методики классификации состояний катастрофоустойчивой системы с использованием гибридной иммунной сети. В рамках данного исследования решены следующие задачи: обоснована значимость обеспечения катастрофоустойчивости информационной системы в процессе управления информационной безопасностью организации в целом; предложен подход к процессу проведения мониторинга и контроля за показателями катастрофоустойчивости системы. Разработана и формально описана гибридная иммунная сеть, с применением алгоритмов клонального и «положительного» отбора и областью покрытия, образованной двумя типами детекторов. Сделан вывод о возможности применения разработанного подхода в процессе анализа катастрофоустойчивости информационных систем.

Катастрофоустойчивость; информационные системы; искусственная иммунная сеть; клональный отбор; «положительный» отбор; мониторинг; информационная безопасность.

V.S. Atkina

MONITORING THE STATES OF INFORMATION SYSTEM DISASTER RECOVERY WITH A HYBRID IMMUNE NETWORK

The purpose of the study is development of technique classification states of disaster recovery systems using a hybrid immune network. This study addressed the following objectives: to substantiate the importance of ensuring disaster recovery information system in the management of information security in general, the approach to the process of monitoring and performance monitoring disaster recovery system. The hybrid immune network is developed and formally described, using algorithms clonal and "positive" selection and coverage area formed by the two types of detectors. The conclusion about possibility of using the developed approach in the analysis of information systems disaster recovery.

Disaster recovery; information system; artificial immune network; positive selection algorithm; clonal algorithm; monitoring; information security.

На сегодняшний день все более необходимым и актуальным для успешного функционирования любой организации вне зависимости от принадлежности ее к государственному или частному сектору экономики является обеспечение непрерывности выполнения ее бизнес-процессов и защита информации от уничтожения, что достигается с помощью информационных систем (ИС) с высокими показателями доступности и катастрофоустойчивости. При этом важным этапов в процессе управления информационной безопасностью организации в целом будет являться деятельность, направленная на проведение периодического и своевременного контроля над текущим состоянием катастрофоустойчивости ИС и выработки по его результатам своевременных катастрофоустойчивых решений, позволяющих скорректировать текущие показатели катастрофоустойчивости.

Для решения задачи контроля за катастрофоустойчивостью ИС как элемента системы управления информационной безопасностью автором предлагается модель системы мониторинга состояний катастрфоустойчивой ИС (КАИС) построенной на базе гибридной иммунной сети, основными функциями которой являются:

- проверка соответствия текущих показателей катастрофоустойчивости КАИС требованиям организации-владельца;
- выявление критичных и наиболее опасных потенциальных катастроф и других дестабилизирующих воздействий существенной среды. [1, 2].

В случае удовлетворения значений показателей катастрофоустойчивости КАИС предъявляемым требованиям и отсутствия критичных для существования КАИС дестабилизирующих факторов (ДФ) существенной среды состояние системы считается «нормальным», в противном случае считается «аномальным», что может свидетельствовать о не удовлетворительных показателях катастрофоустойчивости или низкой способности системы противостоять актуальным для нее ДФ.

В соответствии с подходами к оценки катастрофоустойчивости ИС описанными в работах [3–7] для описания и исследования состояний КАИС предлагается использовать следующие показатели, описанные вектором Sp=(L, T_R, D_{class}, N_{Dlost}, Z), где L – уровень катастрофустойчивости системы; T_R – время восстановления функционирования; D_{class} – класс доступности системы; N_{Dlost} – объем потерянных данных; Z – живучесть. Значения данных показателей вычисляются на основе технико-эксплуатационных характеристик КАИС и данных об имеющихся в ней катастрофоустойчивых решениях. Множество ДФ существенной среды задается множеством DF, где $\forall df_i \in DF$ описывается вектором df_i=(P, U, Risk), где P – вероятность реализации ДФ; U – потенциальный ущерб; Risk – риск.

Формально модель искусственной иммунной сети (ИИС) можно представить следующим образом:

$$IMNet = \{\{ANG^O\}, \{DET^S\}, \{ANG^{DANG}\}, \{ANG^{NORM}\}, ADF, ADS, W_T\}, \quad (1)$$

где $\{ANG^O\}$ – множество образов «антигенов» двух типов $ANG^O = ANG_1^O \cup ANG_2^O$; $\{DET^S\}$ – множество детекторов, представлено двумя типами DET^S и DET^{DF}, при этом $DET = DET^S \cup DET^{DF}$; $\{ANG^{DANG}\}$ – множество потенциально опасных для функционирования системы «антигенов»; $\{ANG^{NORM}\}$ – множество безопасных для функционирования «антигенов»; ADF – матрица аффиностей между образом «антигена» и соответствующим ему типом детектора первого типа; ADS – матрица аффиностей между образом «антигена» и соответствующим ему типом детектора второго типа; W_T – окно сходства.

«Антигены» первого типа ANG_1^O – представляют собой вектор значений, описывающий показатели катастрофоустойчивости Sp, а ANG_2^O – множество ДФ существенной среды.

Детекторы из подмножества DET^S предназначены для распознавания «антигенов» первого типа ANG_1^O, детекторы DET^{DF} – для распознавания «антигенов» ANG_2^O. Посредством сопоставления образов «антигенов» с детекторами иммунная сеть производит классификацию состояний системы. При этом классификатором в общем случае называется функция (формула 2), которая по вектору признаков объекта выносит решение о том, к какому именно классу он принадлежит [8].

$$F : \Re^n \to Y . \quad (2)$$

Функция F отображает пространство векторов признаков в пространство векторов меток Y. В этом случае Y=[0,1], где 0 соответствует «нормальному» состоянию системы, а 1 – «аномальному».

В рамках данной работы предлагается следующий набор шаблонов детекторов, представленных на рис. 1.

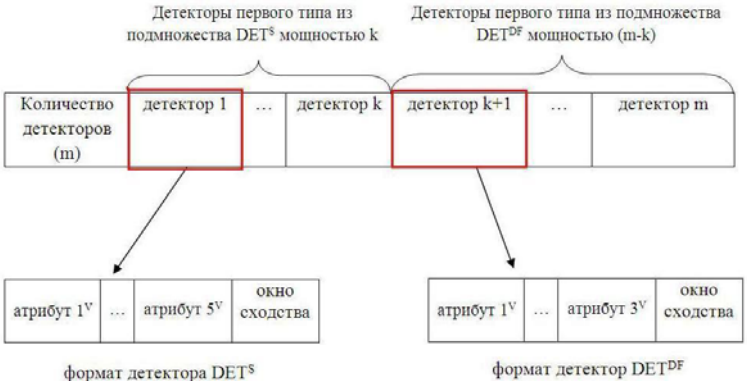

Рис. 1. Формат детекторов иммунной сети

Каждый шаблон детектора имеет следующий формат:

- окно сходства (W) – представляет собой пороговое значение чувствительности детектора (кросс-реактивный порог), зависит от значения степени важности каждого атрибута V. Значение окна сходства W показывает, какие атрибуты в детекторе должны совпасть с соответствующими им значениями анализируемого вектора признаков, чтобы можно было сделать вывод о подобии и принадлежности системы к «нормальному» или «аномальному» состоянию. Например, если W=3, то обязательными должны быть совпадения в тех атрибутах детектора и образа «антигена», которые имеют степень важности V=3;
- атрибуты – значения, по которым осуществляется сопоставление векторов-признаков описывающих состояние системы. Количество атрибутов в каждом детекторе должно быть равно количеству значений в анализируемом векторе;
- степень важности (V) – значение показывающее необходимость совпадения каждого атрибута с соответствующим ему значением в анализируемом векторе признаков.

Детекторы первого типа $det_i^S \in DET^S$, $i=1...k$, где k – количество детекторов, формируются на основе данных множества требований организации-владельца КАИС $R_{DRIS}=\{L^v, T_R^v, D_{class}^v, N_{Dlost}^v, Z^v, T_{DRS}^v, C_{DRS}^v, Risko^v\}$, и могут быть представлены следующим вектором значений атрибутов $det_i^S=(L^v, T_R^v, D_{class}^v, N_{Dlost}^v, Z^v)$.

Детекторы второго типа $det_j^{DF} \in DET^{DF}$, $j=1...(m-k)$, где (m-k) – количество детекторов, формируются на основе данных, описывающих ДФ существенной среды и требований организации-владельца КАИС к предельно допустимому уровню риска $Risko^v$. Данный тип детекторов может быть представлен следующим вектором атрибутов $det_j=(P^v, U^v, Risk^v)$.

При реализации процесса формирования и обучения множества детекторов DET, а так же реализации функции классификации состояний системы, опираясь на решения, описанные в работах [8–10] предлагается использоваться гибридный алгоритм клонального и «положительного отбора».

Детекторы первого и второго типа гибридной иммунной сети осуществляют покрытие множества «своих клеток» при помощи алгоритма клонального «положительного» отбора. В данном случае алгоритм «положительного отбора» предпочтительней использовать по сравнению с «отрицательным» отбором, поскольку он более эффективен в случаях, когда область «чужих клеток» существенно больше области «своих». При этом клональный алгоритм используется в процессе обучения ИИС, а «положительный отбор» – при классификации состояний системы.

При классификации образов «антигенов» первого типа $ang_1^O \in ANG_1^O$ и второго типа $ang_2^O \in ANG_2^O$ в «Т-клетках» с помощью множества детекторов *DET* производится отнесение «антигенов» к одному из двух классов:

$$ANG_{TYPE=1,2}^{DANG} \text{ и } ANG_{TYPE=1,2}^{NORM}.$$

При этом состояние исследуемой КАИС будет считаться «нормальным», если все образы «антигенов» $ANG_{TYPE=1,2}^O$ будут принадлежать классу безопасных для функционирования «антигенов» $ANG_{TYPE=1,2}^{NORM}$, в противном случае состояние системы будет классифицировано как «аномальное», т.е. не советующее требованиям организации-владельца КАИС к показателям катастрофоустойчивости системы и нуждающееся в корректирующих действиях. Используя формулу (2) получим:

$$F(ANG_1^O, ANG_2^O) = \begin{cases} 0, & \text{если } (ANG_1^O \in ANG_1^{NORM}) \text{ и } (ANG_2^O \in ANG_2^{NORM}); \\ 1, & \text{если } (ANG_1^O \in ANG_1^{DANG}) \text{ или } (ANG_2^O \in ANG_2^{DANG}). \end{cases}$$

В процессе классификации иммунная сеть использует правила сопоставления *M*. Так, (det M $ANG_{TYPE=1,2}^O$) определяет аффинность между *det* и $ANG_{TYPE=1,2}^O$, где *det* – детектор, $ANG_{TYPE=1,2}^O$ – входные данные, представленные в виде образа антигена первого или второго типа, подлежащие классификации. Аффинность в данном случае показывает степень соответствия (подобия) между элементом из множества образов «антигенов» каждого типа и соответствующим ему типом детектора.

В качестве правила M определения подобия образов «антигенов» в данной работе предлагается использовать Евклидово расстояние, возможность применения которого обосновано в работе [11]. Для хранения значений вычисленных аффиностей между атрибутами каждого образа «антигена» ang_1^O и сопоставляемым с ним детектором det^S вводится матрица ADF размерностью k×a, где a=5 – количество атрибутов в образе «антигена» первого типа. Для «антигенов» первого типа a=5, k – число детекторов первого типа DET^S. Для хранения аффиностей между «антигенами» второго типа ang_2^O и детекторами $det_i^{DF} \in DET^{DF}, i = 1..z$, вводится матрица ADS размерностью z×b, где b=3 – количество атрибутов в образе «антигена» второго типа и детекторе, z – количество детекторов второго типа DET^{DF}.

Каждый элемент матрицы $ADFij$, представляет собой эвклидово расстояние D_E между атрибутами образа «антигена» и детектора (формула 3):

$$ADFij = D_E = \sqrt[2]{(ang_{1j}^{OV_j} - det_{ij}^{SV_j})^2}. \quad (3)$$

Каждый элемент матрицы $ADSij$, вычисляется по аналогии с формулой 3 и равен:

$$ADSij = D_E = \sqrt[2]{(ang_{21j}^{OV_j} - det_{ij}^{DFV_j})^2}, \quad (4)$$

где V_j – степень важности каждого j атрибута образа «антигена» и детектора соответсвенно.

Атрибуты считаются совпавшими, если выполняется следующее правило:

$$\forall ang_{1j}^{OV_j}, det_{ij}^{SV_j} \mid V_j \geq W_1, ADFij \cong 0;$$
$$\forall ang_{2j}^{OV_j}, det_{ij}^{DFV_j} \mid V_j \geq W_2, ADSij \cong 0, \quad (5)$$

где $W_{T=1,2}$ – окно сходства, $W_T \in \{V\}$. Для определения количества и индексов атрибутов образа «антигена» и детектора, сходство между которыми должно быть обязательным, вводятся множества $LenW_{T=1,2}$ определяющие размер окна сходства W_T, в соответствие со следующим правилом:

$$\forall j \in a | V_j \geq W_1, LenW_1 = LenW_1 \cup \{j\}. \quad (6)$$

$$\forall j \in b | V_j \geq W_2, LenW_2 = LenW_2 \cup \{j\}. \quad (7)$$

Таким образом, все элементы $j_m \in LenW_1,\ m = 1..|LenW_1|$ будут указывать на порядковые номера атрибутов в образе «антигена» первого типа ang_1^O и соответствующими атрибутами детектора det_i^S по которым будет вестись сопоставление, а мощность $|LenW_1| \le a$ на количество атрибутов входящих в окно сходства W_T, см. рис. 2.

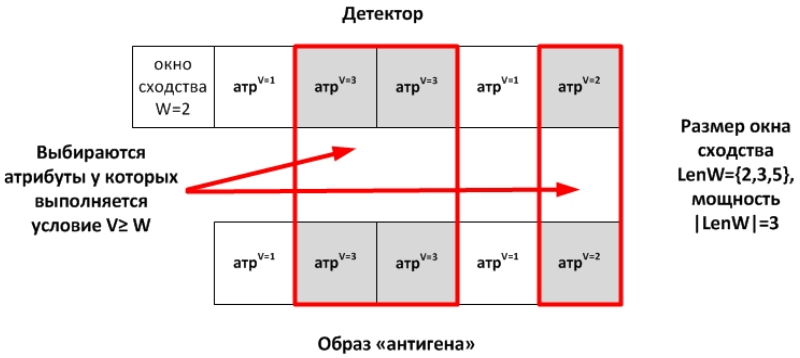

Рис. 2. Формирование окна сходства детектора

Аналогичным образом с использованием (7) формируется множество $LenW_2$ определяющее размер окна сходства и его мощность $|LenW_2| \le b$ для детекторов второго типа.

Общая аффинность между образом «антигена» и i-м детектором представляет собой сумму аффинностей по каждому атрибуту и вычисляется по формуле (9):

$$aff(ang_1^O, det_i^S) = \sum_{j=1}^{a} ADFij$$
$$aff\left(ang_2^O, det_i^{DF}\right) = \sum_{j=1}^{b} ADSij. \quad (9)$$

Образ «антигена» ang_1^O (ang_2^O) считается подобным детектору det_i^S (det_i^{DF}) если выполняется правило максимальной аффиности между образом «антигена» и детектором: $0 \le aff(ang_1^O, det_i^S) \le AFFmax$ ($0 \le aff(ang_2^O, det_i^{DF}) \le AFFmax$).

Пороговое значение аффинности $AFFmax$ выбирается исходя из условия:

$$AFFmax = \min_{\substack{D_{Ej(k)} \to 0, \\ \forall j \in LenW}} \left(\sum_{k=1}^{|LenW|} D_{Ej(k)} \right)$$

В общем виде процесс классификации состояния КАИС по векторам – признаков двух типов на основе алгоритма «положительного отбора» (см. рис. 3) можно описать в виде следующего алгоритма действий:

1. Инициализируем иммунную память и формируем множество детекторов DET. Детекторы первого типа DET^S реагируют на образы «антигенов» первого типа ANG_1^O. Детекторы второго типа DET^{DF} – на «антигены» второго типа ANG_2^O. При этом считаем, что $DET=DET^S \cup DET^{DF}$.

2. Для каждого элемента $ang_1^O \in ANG_1^O$ и $ang_2^O \in ANG_2^O$ выполняем этапы.

3. Вычисляем аффинность между детекторами первого и второго типа и соответствующими им образами «антигенов»: $aff(ang_1^O, det^s)$, $aff(ang_2^O, det^{DF})$. Считаем, что правило М выполняется, когда значение аффинности ниже порогового, т.е. когда det^s и ang_1^O, det^{DF} и ang_2^O достаточно подобны.

4. Для тех элементов из множества образов «антигенов» первого типа $ang_1^O \in ANG_1^O$ для которых выполняется правило $(ang_1^O\ M\ det^S)$ производим их

включение во множество безопасных для функционирования КАИС антигенов ANG_1^{NORM}: $ANG_1^{NORM} = ANG_1^{NORM} \cup \{ang_1^O\}$, $ANG_1^O = ANG_1^O \backslash \{ang_1^O\}$, и производим процедуру обучения ИМС путем расширения множества детекторов DET^S: $DET^S = DET^S \cup \{ang_1^O\}$ и увеличением области покрытия. В противном случае элемент ang_1^O классифицируется как опасный для функционирования и перемещается в множество антигенов ANG_1^{DANG}: $ANG_1^{DANG} = ANG_1^{DANG} \cup \{ang_1^O\}$, $ANG_1^O = = ANG_1^O \backslash \{ang_1^O\}$.

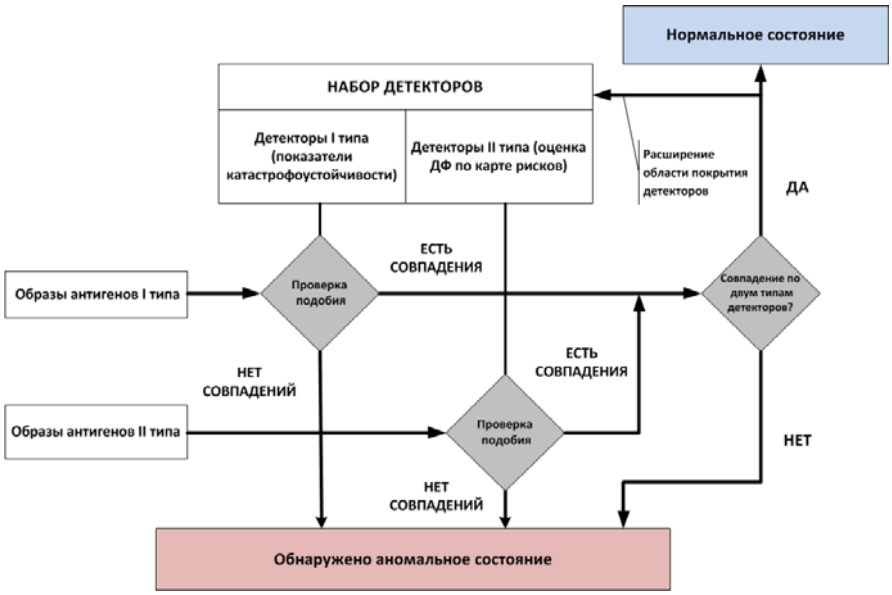

Рис. 3. Схема процедуры классификации гибридной иммунной сети

5. Аналогичным образом, в случае выполнения правила (ang_2^O *M det*^{DF}) производим перемещение элементов ang_2^O из множества образов «антигенов» второго типа ANG_2^O во множество безопасных для состояния КАИС антигенов ANG_2^{NORM}: $ANG_2^{NORM} = ANG_2^{NORM} \cup \{ang_2^O\}$, $ANG_2^O = ANG_2^O \backslash \{ang_2^O\}$. Производим процедуру обучения ИМС путем расширения множества детекторов DET^{DF}: $DET^{DF} = DET^{DF} \cup \{ang_2^O\}$ и увеличением области покрытия. В противном случае элемент ang_2^O классифицируется как опасный для функционирования и перемещается во множество антигенов ANG_2^{DANG}: $ANG_2^{DANG} = ANG_2^{DANG} \cup \{ang_2^O\}$, $ANG_2^O = ANG_2^O \backslash \{ang_2^O\}$.

6. Проверяем множества ANG_1^{NORM}, ANG_2^{NORM}, ANG_2^{DANG}, ANG_1^{DANG} на наличие пустых элементов.

7. Если выполняется условие, что множество классов безопасных для функционирования системы «антигенов» не пустые, а классы опасных антигенов не содержат элементов, то характеристическая функция $F(ANG_1^O, ANG_2^O) = 0$ и состояние системы классифицируется ИИС как «нормальное».

8. Во всех остальных случаях состояние системы классифицируется ИИС как «аномальное» $F(ANG_1^O, ANG_2^O) = 1$.

Предложенный подход реализован программно в составе подсистемы комплекса по управлению процессом анализа катастрофоустойчивости ИС и принятием катастрофустойчивых решений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Atkina V.S.* Semantic model of disaster recovery information system // European Science and Technology: international scientific conference/ Bildungszentrum Rdk e.V. – Wiesbaden, Germany 2012. – P. 162-164.
2. *Машкина И.В. Сенцова А.Ю. Гузаиров Р.М. Кладов В.Е.* Использование методов системного анализа для решения проблемы обеспечения безопасности современных информационных систем // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 25-35.
3. *Беленков В.Г. Будзко В.И. Синицын И.Н.* Катастрофоустойчивость корпоративных информационных систем. Ч. 1. – М.: ИПИ РАН, 2002.
4. *Будзко В.И.* Количественные оценки отказоустойчивых и катастрофоустойчивых решений // Вопросы защиты информации. – 2003. – № 2. – С. 19-32.
5. Аткина В.С. Живучесть системы как показатель ее катастрофоустойчивости // Проблемы обеспечения информационной безопасности в регионе : материалы III Регион. науч.-практ. конф., г. Волгоград, 20 апр. 2010 г. – Волгоград: Изд-во ВолГУ, 2010. – С. 42-57.
6. *Павлов А.Н. , Соколов Б.В.* Структурный анализ катастрофоустойчивой информационной системы //Труды СПИИРАН. Вып. 8. – М., 2009. – С. 128-153.
7. *Аткина В.С.* Подходы к оценке катастрофоустойчивости ИС// Проблемы модернизации региона в исследованиях молодых ученых: Материалы VI Межрегион. науч.-практ. конф., г. Волгоград, 30-31 марта 2010. – Волгоград: Изд-во ВолГУ, 2010. – С. 356-357.
8. *Литвиненко В.И., Дидык А.А., Фефелов А.А., Херсон.* Модифицированный гибридный иммунный алгоритм на основе теорий отрицательного и клонального отбора для решения задач классификации и его программная реализация // Моделирование информационных технологий. Вып. 62. – Киев, 2011. – С. 86-94.
9. *Зайцев С.А., Субботин С.А.* Обобщенная модель искусственной иммунной сети // Нейроинформатика. Ч. 2. – 2010. – С. 98-107.
10. Оладько А.Ю. Модель адаптивной многоагентной системы защиты в ОС Solaris 10 // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 210-217.
11. *Bidyuk P.I., Litvinenko V.I., Gasanov A.S.* Immune network based method for identification of turbine engine surging // Кафедра математического и системного анализа: [сайт]. URL – http://www.mmsa.kpi.ua. (дата обращения 10.09.2012).

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Аткина Владлена Сергеевна – Волгоградский государственный университет; e-mail: atkina.vlaldlena@yandex.ru; 400062, г. Волгоград, пр-т Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; старший преподаватель.

Atkina Vladlena Sergeevna – Volgograd State University; e-mail: atkina.vlaldlena @ yandex.ru; 100, University avenue, Volgograd, 400062, Russia; phone: +78442460368; the department of information security; senior lecturer.

УДК 004.942

Д.А. Ляшко, И.В. Аникин

МОДЕЛИРОВАНИЕ АГЕНТА И МЕНЕДЖЕРА СИСТЕМЫ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Целью работы является повышение эффективности защиты автоматизированных систем от несанкционированного доступа (НСД) за счет централизации управления функциями по защите информации от НСД. В работе определен состав компонентов и разработана структура системы централизованного удаленного администрирования средствами защиты информации от НСД (СУДАД-ЗИ), разработаны формальные математические