УДК 004.056

СИСТЕМНЫЙ АНАЛИЗ МОДЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ ВЛИЯЮЩЕЙ НА ОЦЕНКУ ЭФФЕКТИВНОСТИ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ

Власенко Александра Владимировна
Кандидат технических наук, доцент, доцент кафедры компьютерных технологий и информационной безопасности института компьютерных систем и информационной безопасности, начальник управления аспирантуры и докторантуры
ФГБОУ ВПО "Кубанский государственный технологический университет"
тел. 89184482931, Vlasenko@kubstu.ru

Чебанов Александр Сергеевич
аспирант института компьютерных систем и информационной безопасности
ФГБОУ ВПО "Кубанский государственный технологический университет"
тел. 89676666006, ascheb9@mail.ru

В статье представлена разработка математической модели управления правами доступа влияющей на оценку эффективности комплексных систем защиты путем отбора факторов, а так же групп факторов влияющих на политику безопасности системы. Модель работает путем формирования бинарных выражений, результатом которых будет либо нулевое значение, либо единица, либо не существенное значение. Далее объект управления производит сравнение и анализ полученных значений и выдает экспертное решение блокирования прав доступа, либо нет. Данная система адаптивна и способна развиваться, путем добавления различных факторов и расширения экспертных решений

Ключевые слова: МОДЕЛЬ БЕЛЛА-ЛАПАДАЛЫ, МАНДАТНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ, БИНАРНАЯ ФУНКЦИЯ, ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ЗАЩИТУ ИНФОРМЦИИ, НСД, ИНФОРМАЦИОННЫЙ ПОТОК

UDC 004.056

SYSTEM ANALYSIS OF MODELS OF INFORMATION SECURITY, THE DEVELOPMENT OF A MATHEMATICAL MODEL OF ACCESS CONTROL WHICH AFFECTS THE EVALUATION OF THE EFFECTIVENESS OF THE INTEGRATED SYSTEMS OF PROTECTION

Vlasenko Aleksandra Vladimirovna
Candidate of engineering sciences, associate professor, associate professor of department of computer technologies and informative safety of institute of information technologies and safety, chief of management of postgraduate and doctorate

Kuban state technological university, Krasnodar, Russia
tel. 89184482931, **Vlasenko@kubstu.ru**

Chebanov Aleksandr Sergeevich
postgraduate student of institute of information technologies and safety
Kuban state technological university, Krasnodar, Russia
tel. 89676666006,ascheb9@mail.ru

The article describes a development of the mathematical model for managing access rights affecting the assessment of the effectiveness of the integrated systems of protection with selection factors, as well as groups of factors affecting the system security policy. The model works due to forming a binary expression which would lead to either a zero value or the unit, or not significant value. Next, we have control comparisons and analysis of the values that provides an expert decision about blocking the access rights or not. This system is adaptive and able to evolve by adding various factors and expansion of expert decisions

Keywords: MODEL OF BELLA LAPADALY, CREDENTIALS ACCESS CONTROL MODEL, BINARY FUNCTION, FACTORS AFFECTING INFORMATION PROTECTION, TAMPER, INFORMATION FLOW

В настоящее время широко развито направление разработки моделей управления доступом. Не секрет что модель управления доступом – это весьма значимая составляющая системы безопасности в целом и от её функциональной работы будет зависеть эффективность всей системы

безопасности в комплексе. Однако, подавляющее большинство моделей безопасности строго регламентированы, очень громоздки либо требуют больших трудозатрат и финансовых вложений. Целью разработки настоящей модели была минимизация вышеперечисленные недостатков существующих моделей и как следствие повышение эффективности комплексных систем безопасности.

Модель управления доступом рис.1 включает в себя все достоинства модели Белла-Лападулы [1-2] , но в отличие от строго регламентированной модели Б-Л, в чем и заключается основное преимущество данной модели – это адаптивность, то есть модель функционирует динамически, анализирует влияющие на нее факторы, рычаги воздействия со стороны суперпользователя (при нестандартных ситуациях) и оперативно реагирует, блокируя потоки информации между субъектами и объектами от уровней с более высокой секретностью к уровням с более низкой секретностью.

Модель системы управления доступом на рисунке 1 позволяет увидеть информационные потоки 1 – 4, по средствам которых происходит обмен информацией между высоким уровнем секретности и низким уровнем секретности. На рисунке 1 информационные потоки не ограниченны ни в одном из направлений обмена, это создает большую угрозу утечки, искажения, нарушения доступности к информации, а так же ее потери [3].

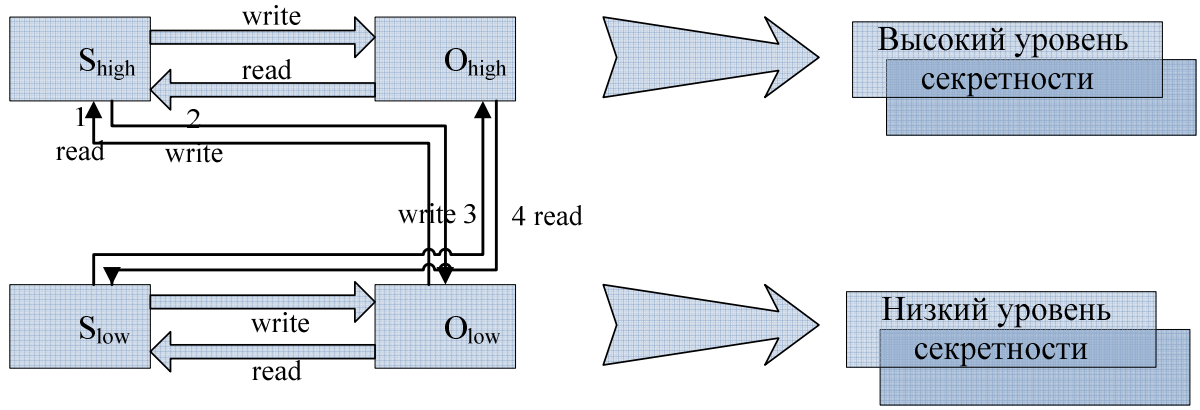

Рисунок 1 – модель управления доступом без ограничения доступа к информации

Как известно из формального описания, модель Белла-Лападула вводит ограничения по чтению информации для пользователей нижнего уровня, но разрешает таким пользователям запись информации в верхний уровень секретности и наоборот пользователям высокого уровня секретности не разрешается запись секретной информации вниз, но возможность чтения информации нижнего уровня присутствует. Казалось бы, модель идеальна и без изъянов, но строгое соответствие правилам и не возможность адаптироваться к различным внешним и внутренним факторам, не минуемо возникающих в системе в большинстве случаев отрицательным образом влияющих на работу системы, рано или поздно, однозначно приведет к сбою системы и, как следствие, утечки информации.

Фактор, воздействующий на защищаемую информацию – явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней; [4]

На штатную работу модели, на ее надежность и стабильное функционирование внутри системы оказывают влияние совокупность факторов. Всё многообразие факторов влияющих на объект информатизации, в том числе на надежность модели и как следствие является средоточием возникновения угроз на объекте информатизации, делятся на несколько категорий, к которым относятся физические, физико-химические, эксплуатационные факторы и многие другие. Для простоты мы объединим их в 2 категории: внутренние и внешние факторы [5].

$$F = F_{внут} \cup F_{внеш}; \quad (1)$$

где $F_{внут}$ – совокупность внутренних факторов;

где $F_{внеш}$ – совокупность внешних факторов;

Для удобства представления, для большей наглядности, а так же для гибкости и возможности расширения списка факторов влияющих на систему, занесем их в таблицу.

Таблица 1 – Совокупность факторов оказывающих влияние на модель зависящих от номера информационного потока

Общие Факторы		$F_{№1}$	$F_{№2}$	$F_{№3}$	$F_{№4}$
$F_{внутр}$	$F_{внеш}$	$F_{1,1}$	$F_{2,1}$	$F_{3,1}$	$F_{4,1}$
F_1	F_2	$F_{1,2}$	$F_{2,2}$	$F_{3,2}$	$F_{4,2}$
F_3	F_4	$F_{1,3}$	$F_{2,3}$	$F_{3,3}$	$F_{4,3}$
F_5	F_6	$F_{1,4}$	$F_{2,4}$	$F_{3,4}$	$F_{4,4}$
F_7	F_8	$F_{1,5}$	$F_{2,5}$	$F_{3,5}$	$F_{4,5}$
…	…	…	…	…	…
F_K	F_G	$F_{1,N}$	$F_{2,M}$	$F_{3,L}$	$F_{4,Q}$

Рассмотренные в таблице 1 категории факторов были разделены в зависимости от информационных потоков, пронумерованных на рисунке 9. Если осуществляется доступ на чтение (read) субъекта S к объекту O, то поток информации идет от O к S – поток информации номер 1. Если S имеет доступ на запись (write) к O, то информационный поток направлен от S к O – номер 2. Аналогично и с информационными потоками номер 3 и 4. Транзитивное замыкание цепочек доступа (даже без учета времени) представляет собой сложный информационный поток. Однако мы остановимся на том, что замыкание цепочек доступа будет зависеть в первую очередь от факторов, возникающих в процессе функционирования системы.

Заметим, что множество факторов в общем виде, в зависимости от информационного потока, можно показать следующим выражением 2:

$$F = F_{внут} \cup F_{внеш} \cup F_{№1} \cup F_{№2} \cup F_{№3} \cup F_{№4} \cup \ldots, \quad (2)$$

где,

$$F_{внут} = \{F_1, F_3, F_5, F_7 \ldots F_K\} \quad (3)$$

$$F_{внеш} = \{F_2, F_4, F_6, F_8 \ldots F_G\} \quad (4)$$

$$F_{№1} = \{F_{1,1}, F_{1,2}, F_{1,3}, F_{1,4} \ldots F_{1,N}\} \quad (5)$$

$$F_{№2} = \{F_{2,1}, F_{2,2}, F_{2,3}, F_{2,4} \ldots F_{2,M}\} \quad (6)$$

$$F_{№3} = \{F_{3,1}, F_{3,2}, F_{3,3}, F_{3,4} \ldots F_{3,L}\} \quad (7)$$

$$F_{№4} = \{F_{4,1}, F_{4,2}, F_{4,3}, F_{4,4} \ldots F_{4,Q}\} \quad (8)$$

При необходимости совокупность групп факторов можно дополнить и это ни как не повлияет на фундаментальную идею модели, тем самым модель приобретает возможность совершенствования и развития, ведь прогресс не стоит на месте.

Для большего понимания предмета исследования покажем влияние факторов на конкретном примере из совокупности нескольких факторов по всем шести группам из рассмотренных выше выражений 3 – 8.

1. Чтение объекта с низким уровнем секретности $\mathbf{O_{low}}$ субъектом с высоким уровнем доступа $\mathbf{S_{high}}$.

Факторы этой группы носят сугубо специфический характер, поскольку система безопасности нашей модели реагирует на них, если таковые возникают исключительно при взаимодействии субъекта и объекта в информационном потоке под номером 1 исходя из таблицы 3. Итак, распишем несколько факторов для наглядности:

$F_{1,1}$ – Копирование файла с высокого уровня секретности на низкий (вывод информации на периферийные устройства);

$F_{1,2}$ – Обнаружение вируса;

2. Запись объекта с низким уровнем секретности $\mathbf{O_{low}}$ субъектом с высоким уровнем доступа $\mathbf{S_{high}}$.

$F_{2,1}$ – Несанкционированное изменение информации;

$F_{2,2}$ – Обнаружение вируса, сбой/отключение антивирусной программы;

3. Запись объекта с высоким уровнем секретности $\mathbf{O_{high}}$ субъектом с низким уровнем доступа $\mathbf{S_{low}}$.

$F_{3,1}$ – Несанкционированное изменение информации;

$F_{3,2}$ – Обнаружение вируса, сбой/отключение антивирусной программы;

4. Чтение объекта с высоким уровнем секретности $\mathbf{O_{high}}$ субъектом с низким уровнем доступа $\mathbf{S_{low}}$.

$F_{4,1}$ – Обнаружение вируса;

$F_{4,2}$ – Несанкционированный доступ (попытка НСД) к защищаемой информации, доступ к которой отсутствует у данного пользователя;

$F_{4,3}$ – Копирование файла с низкого уровня на высокий (вывод информации на периферийные устройства);

Факторы общей группы, учитывающиеся при взаимодействии всех информационных потоков.

F_1 – Нарушение функционирования аппаратной части ПК;

F_2 – Использование запрещенного ПО на ПК, несоответствующего политике информационной безопасности;

F_3 – Сбои, отказы и аварии обеспечении питания;

F_4 – Несанкционированное копирование информации;

F_5 – Копирование информации на незарегистрированный носитель информации;

F_7 – Сбои, ошибки, отказы в работе при эксплуатации ТС, ПО, средств и систем ЗИ;

F_8 – Использование программных закладок, т.е. внесение изменение в функционал программы;

F_9 – Несоблюдение требований по защите информации;

F_{10} – разглашение информации лицам, не имеющим права доступа к защищаемой информации;

Исходя из вышеописанной системы влияния факторов на политику функционирования разрабатываемой модели безопасности, можно описать

взаимодействие субъектов S с объектами O следующими выражениями опираясь на номера информационного потока. Итак, взаимодействие субъектов и объектов первого потока определяется бинарной функцией, результатом которой будет значение равное либо нолю, либо единицы:

$$\omega_{1,1}(F) = \overline{F_1} \,\&\, \overline{F_2} \,\&\overline{F_3} \,\&\, \overline{F_5} \,\&\overline{F_7} \,\&\overline{F_8} \,\&\overline{F_9} \,\&\overline{F_{1,1}} \,\&\overline{F_{1,2}} \;; (9)$$

Логическое умножение бинарной функции 9, показывающая значение для первого информационного потока, как было сказано выше, в результате даст одно из двух возможных значений: если появляется хотя бы один из факторов, в процессе функционирования системы, общее значение функции будет равно единицы, это даст команду в объект управление на блокирование информационного потока под номером 1 (рисунок 2), если в процессе работы системы значение бинарной функции равно нолю, это означает, что какие-либо факторы влияющие на политику безопасности системы отсутствуют и обмен информации в данном информационном потоке открыт и происходит в штатном режиме.

Взаимодействие субъектов и объектов второго информационного потока:

$$\omega_{2,1}(F) = \overline{F_1} \,\&\, \overline{F_2} \,\&\overline{F_3} \,\&\overline{F_4} \,\&\overline{F_5} \,\&\overline{F_7} \,\&\overline{F_8} \,\&\overline{F_9} \,\&\overline{F_{2,1}} \,\&\overline{F_{2,2}} \;; (10)$$

В данном выражении помимо общих факторов, влияющих на систему, имеют место быть специфические для второго информационного потока факторы, наличие которых опять же заблокирует обмен информацией по доступным правам во втором информационном потоке.[6]

Бинарная функция взаимодействие субъектов и объектов третьего информационного потока будет иметь следующее выражение:

$$\omega_{3,1}(F) = \overline{F_1} \,\&\, \overline{F_2} \,\&\overline{F_3} \,\&\overline{F_4} \,\&\overline{F_5} \,\&\overline{F_7} \,\&\overline{F_8} \,\&\overline{F_9} \,\&\overline{F_{3,1}} \,\&\overline{F_{3,2}} \;; (11)$$

Заключительная функция взаимодействие субъектов и объектов четвертого информационного потока:

$$\omega_{4,1}(F) = \overline{F_1} \,\&\, \overline{F_2} \,\&\overline{F_3} \,\&\overline{F_4} \,\&\overline{F_5} \,\&\overline{F_7} \,\&\overline{F_8} \,\&\overline{F_9} \,\&\overline{F_{4,1}} \,\&\overline{F_{4,2}} \,\&\overline{F_{4,3}}\ ; (12)$$

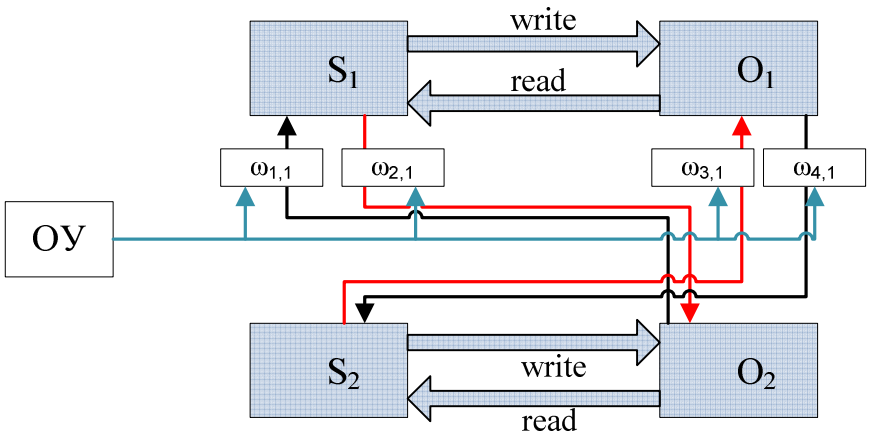

Рисунок 2 – Модель управления доступом основанная на объекте управления и бинарных функциях

Данные выражения 9 – 12 отражают отношение между субъектами и объектами первого и второго уровней, применительно к модели это можно увидеть на рисунке 2. Таких уровней может быть неограниченное количество. Пусть, к примеру, их будет i-е множество.

Тогда предпоследнее выражение функции взаимодействия субъектов и объектов с первого по четвертый информационные потоки примет вид:

$$\omega_{1,i-1}(F) = \overline{(F_1 \& F_2 \& F_3 \& \dots \& F_K \& F_G)} \,\&\overline{(F_{1,1} \& F_{1,2} \& \dots \& F_{1,N}}\ ; (13)$$

$$\omega_{2,i-1}(F) = \overline{(F_1 \& F_2 \& F_3 \& \dots \& F_K \& F_G)} \,\&\overline{(F_{1,1} \& F_{1,2} \& \dots \& F_{1,N}}\ ; (14)$$

$$\omega_{3,i-1}(F) = \overline{(F_1 \& F_2 \& F_3 \& \dots \& F_K \& F_G)} \,\&\overline{(F_{1,1} \& F_{1,2} \& \dots \& F_{1,N}}\ ; (15)$$

$$\omega_{4,i-1}(F) = \overline{(F_1 \& F_2 \& F_3 \& \dots \& F_K \& F_G)} \,\&\overline{(F_{1,1} \& F_{1,2} \& \dots \& F_{1,N}}\ ; (16)$$

Исходя из выражений 13 – 16 можно сделать вывод, что факторов может быть бесчисленное множество, конечно же для начала необходимо потратить какое-то время для описания факторов и их влияния на комплексную систему безопасности в целом, но результат должен окупить себя.

Не оставлена без внимания иерархия управления модели. Если взглянуть на рисунок 3 , то можно понять, что каждый последующий

уровень доступа к секретной информации субъекта и объекта будет ниже уровня доступа предшествующих субъектов и объектов:

$$S_1 > S_2 > \ldots S_{i-1} > S_i ;$$

$$O_1 > O_2 > \ldots O_{i-1} > O_i ;$$

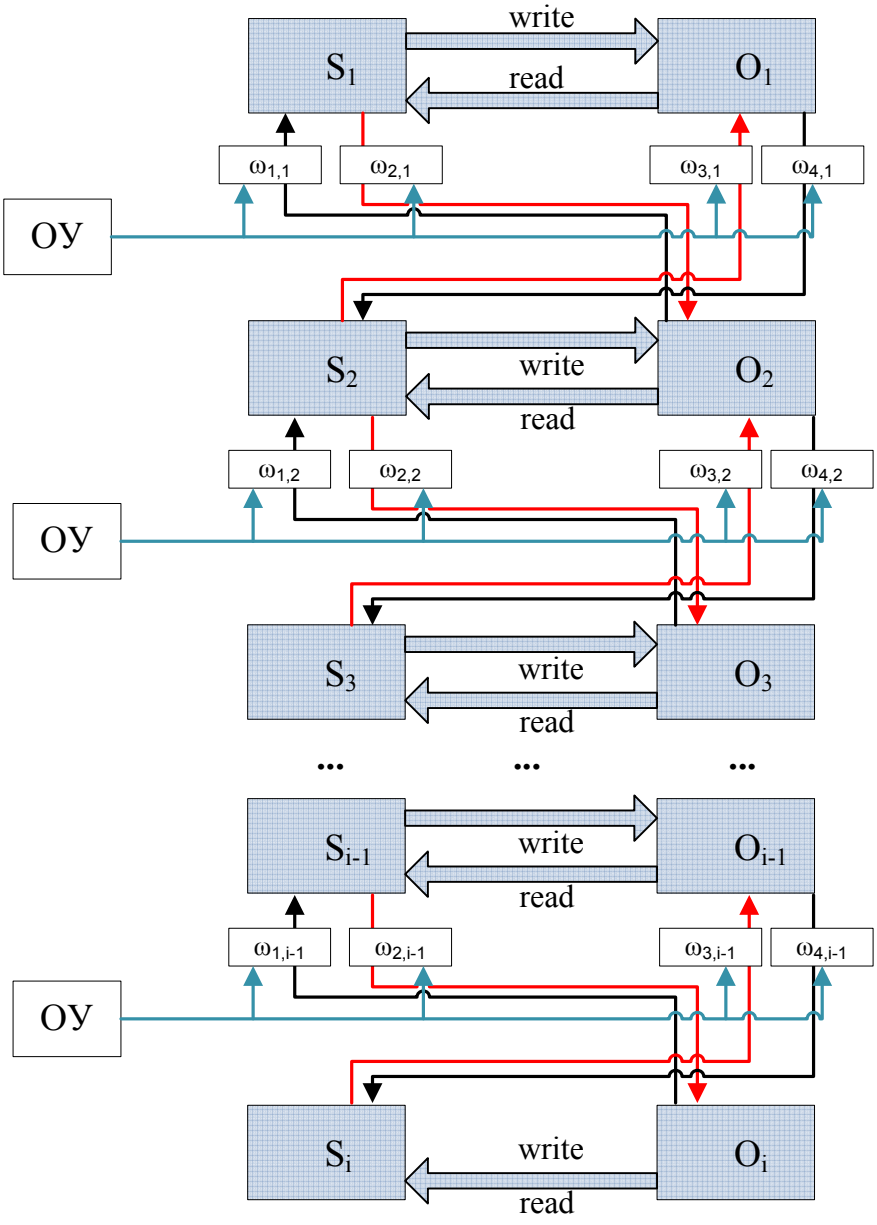

Рисунок 3 – Модель управления доступом основанная на объекте управления и бинарных функциях в i-мерном виде

Результат, полученный путем решения бинарных функций 9 – 12, либо 13 – 16 переходит на следующий этап функционирования модели управления доступом.

Объект управления передает выходящий из функций 9 – 12 результат в управляющую систему следующего вида:

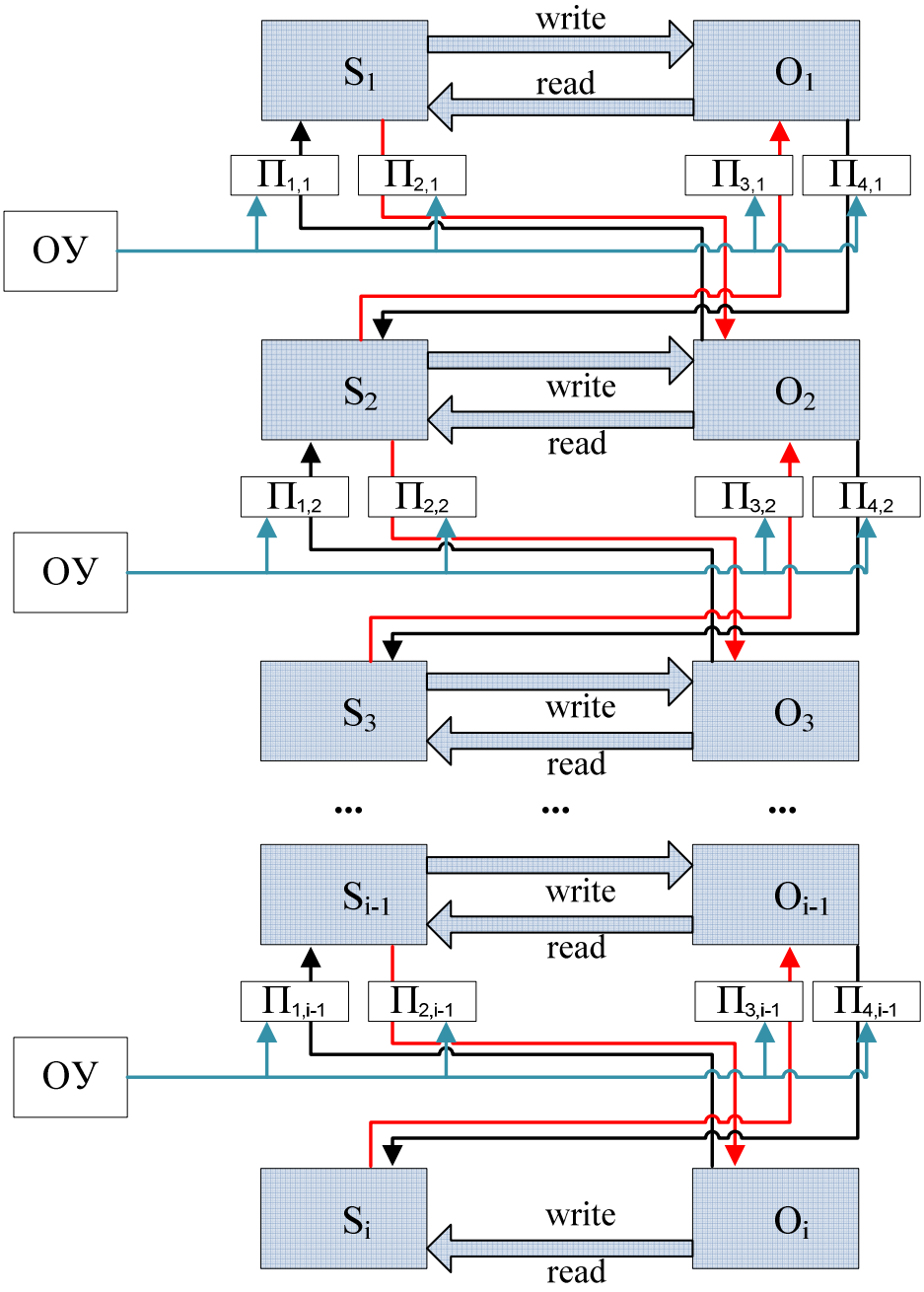

Рисунок 4 – Модель управления доступом основанная на функциях с учетом экспертных правил в i-мерном виде

$$\Pi_{1,1} = \begin{cases} \omega_{1,1}, & F_0 = \text{н.с.} \\ 0, & F_0 = 0\ (f) \\ \omega_{1,1}, & F_0 = 1\ (t) \end{cases} \qquad \Pi_{2,1} = \begin{cases} \omega_{2,1}, & F_0 = \text{н.с.} \\ 0, & F_0 = 0\ (f) \\ \omega_{2,1}, & F_0 = 1\ (t) \end{cases}$$

$$\Pi_{3,1} = \begin{cases} \omega_{3,1}, & F_0 = \text{н.с.} \\ 0, & F_0 = 0\ (f) \\ \omega_{3,1}, & F_0 = 1\ (t) \end{cases} \qquad \Pi_{4,1} = \begin{cases} \omega_{4,1}, & F_0 = \text{н.с.} \\ 0, & F_0 = 0\ (f) \\ \omega_{4,1}, & F_0 = 1\ (t) \end{cases} \qquad (17)$$

Для сравнения результатов бинарных функций полученных из выражений 13 – 16 система примет следующий вид:

$$\Pi_{1,i-1} = \begin{cases} \omega_{1,i-1}, & F_0 = \text{н.с.} \\ 0, & F_0 = 0\ (f) \\ \omega_{1,i-1}, & F_0 = 1\ (t) \end{cases} \qquad \Pi_{2,i-1} = \begin{cases} \omega_{2,i-1}, & F_0 = \text{н.с.} \\ 0, & F_0 = 0\ (f) \\ \omega_{2,i-1}, & F_0 = 1\ (t) \end{cases}$$

$$\Pi_{3,i-1} = \begin{cases} \omega_{3,i-1}, & F_0 = \text{н.с.} \\ 0, & F_0 = 0\ (f) \\ \omega_{3,i-1}, & F_0 = 1\ (t) \end{cases} \qquad \Pi_{4,i-1} = \begin{cases} \omega_{4,i-1}, & F_0 = \text{н.с.} \\ 0, & F_0 = 0\ (f) \\ \omega_{4,i-1}, & F_0 = 1\ (t) \end{cases} \qquad (18)$$

где, $F_0 = \{f, t, \text{н.с.}\}$,

где, н.с. – несущественное значение. То есть если, к примеру, существует отдельная группа факторов, возникновение которых не оказывает особого влияния на политику безопасности системы комплексной защиты, то такой фактор, либо группа факторов принимают несущественное значение;

где, f = 0 , то есть функция Π принимает значение равное нулю, если бинарная функция ω принимает нулевое значение, а именно при отсутствии факторов, влияющих на систему;

где, t = 1 , то есть функция Π принимает значение равное единицы, если бинарная функция ω принимает значение единицы, а именно если присутствует хотя бы один фактор, влияющий на систему;

Итак, когда значение из функций 9 – 12 попадает в систему анализа и сравнения результатов, так называемый объект управления, то на этом заключающем этапе происходит сравнение полученных данных и затем на выходе получаем соответствующее значение в виде экспертного решения. Если в функцию $П_{1.1}$ попадает значение $\omega_{1.1} = 0$, функция $П_{1.1}$ выдает результат false, т.е. система работает в штатном режиме. Если же в функцию $П_{1.1}$ попадает значение $\omega_{1.1} = 1$, функция $П_{1.1}$ выдает результат true, т.е. на систему оказывает влияние не желательный фактор, последующее действие блокирует информационный поток под номером один, т.е. права на чтение объекта с низким уровнем секретности $\mathbf{O_{low}}$ субъектом с высоким уровнем доступа $\mathbf{S_{high}}$ отсутствуют пока нежелательный фактор не будет удален.

ЛИТЕРАТУРА

Информационная безопасность: учебное пособие / В.А. Семененко. Москва: Московский государственный индустриальный университет, 2010.-277с.

Основы информационной безопасности автоматизированных систем: краткий курс / В.Л. Цирлов. Феникс,2008.-173с.

Информационная безопасность: учебное пособие / С.И. Макаренко. Ставрополь: СФ МГТУ им. М.А. Шолохова, 2009. – 372с.

ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию.

Надежность информационных систем: учебное пособие / Ю.Ю. Громов, О.Г. Иванов, Н.Г. Мосягина, К.А. Набатов. Тамбов: Издательство ГОУ ВПО ТГТУ, 2010 – 160 с.

Системный анализ: учебник для ВУЗов / А.В. Антонов. Москва: Высшая школа, 2004. – 454 с.

References

1. Informacionnaja bezopasnost': uchebnoe posobie / V.A. Semenenko. Moskva: Moskovskij gosudarstvennyj industrial'nyj universitet, 2010.-277s.

2. Osnovy informacionnoj bezopasnosti avtomatizirovannyh sistem: kratkij kurs / V.L. Cirlov. Feniks,2008.-173s.

3. Informacionnaja bezopasnost': uchebnoe posobie / S.I. Makarenko. Stavropol': SF MGTU im. M.A. Sholohova, 2009. – 372s.

4. GOST R 51275-2006 Zashhita informacii. Ob#ekt informatizacii. Faktory, vozdejstvujushhie na informaciju.

5. Nadezhnost' informacionnyh sistem: uchebnoe posobie / Ju.Ju. Gromov, O.G. Ivanov, N.G. Mosjagina, K.A. Nabatov. Tambov: Izdatel'stvo GOU VPO TGTU, 2010 – 160 s.

6. Sistemnyj analiz: uchebnik dlja VUZov / A.V. Antonov. Moskva: Vysshaja shkola, 2004. – 454 s.