УДК 681.3

М.В. Буйневич, А.А. Емельянов

МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ОТ НСД К КРИТИЧЕСКИМ ИНФОРМАЦИОННЫМ РЕСУРСАМ ПРИ ПРОЕКТИРОВАНИИ АСУ

***Буйневич Михаил Викторович**, кандидат технических наук, окончил Высшее военно-морское училище радиоэлектроники им. А.С. Попова. Профессор 3-го факультета ВМИРЭ им. А.С. Попова. Имеет монографии, статьи, учебники и учебные пособия в области автоматизации систем управления ВМФ. [Тел.: (812) 427-10-11].*

***Емельянов Александр Алексеевич**, кандидат технических наук, окончил Военную академию им. Ф.Э. Дзержинского. Заместитель генерального директора по качеству, эффективности и инженерно-техническому обеспечению ФНПЦ ОАО «НПО «Марс» - начальник управления. Имеет публикации в области создания систем менеджмента качества и защиты информации. [E-mail: mars@mv.ru].*

Аннотация

Разработан алгоритм функционирования системы защиты информации (СЗИ) от несанкционированного доступа (НСД), реализующий заданный перечень функций с учетом введенных допущений. На основе алгоритма построена математическая модель системы защиты с оптимизацией времени и стоимости реализации отдельных запросов.

Ключевые слова: система защиты информации (СЗИ), защита информации при проектировании АСУ, математическая модель системы защиты, алгоритм функционирования СЗИ, критические информационные ресурсы, автоматическая система боевого управления (АСБУ).

Abstract

The article deals with an algorithm developed to ensure the operation of a system of information protection against unauthorized access, which implements a given function list taking into account introduced assumptions. The mathematical model of the protection system is designed on basis of the algorithm taking into account optimization of time and cost of implementation of some requests.

Key words: information security system, information security during C2 system design, mathematical model of system protection, algorithm of information security system operation, critical information resources, computer-aided combat management system.

Обеспечение защиты информации, циркулирующей в процессе проектирования АСУ, является одной из наиболее актуальных задач, без решения которой само проектирование может стать бессмысленным.

Основными задачами системы защиты информации являются:

- своевременное выявление и предотвращение утечки информации по техническим каналам;
- исключение или существенное затруднение несанкционированного доступа к информации, хищения технических средств и носителей информации;
- предотвращение воздействий, вызывающих нарушение целостности информации или работоспособности.

В РФ требования к системам комплексной защиты информации формируются, главным образом, на основе руководящих документов Государственной технической комиссии (РД ГТК).

Требования к СЗИ от НСД, изложенные в РД ГТК в виде необходимого и достаточного перечня функций, являются основой для алгоритмизации ее функционирования [1-3]. Однако указанный перечень необходимо дополнить рядом допущений.

Первое связано с необходимостью заполнения пауз информационно-вычислительного процесса самоконтролем СЗИ от НСД: обращение к задачам тестового контроля происходит всякий раз, когда запрос или заявка на решение прикладной или системной задачи в автоматизированной системе проектирования (АСП) оказывается последней.

Второе обязывает делить всю информацию в АСП как минимум на две группы по степени ее конфиденциальности: информация с миниманль-

ным уровнем конфиденциальности и «закрытая» информация. Такое деление вызвано различием набора функций, выполняемых СЗИ от НСД для каждой из групп.

Третье связано с возможностью адаптивного управления СЗИ и предполагает динамический выбор метода реализации функций, например, вторичной идентификации пользователя при доступе к критическим информационным ресурсам (КИР). Возможность динамического выбора той или иной функции определяется РД ГТК.

Дифференциация доступа к «закрытой» информации сопряжена с выполнением ряда дополнительных функций. Здесь требуется так

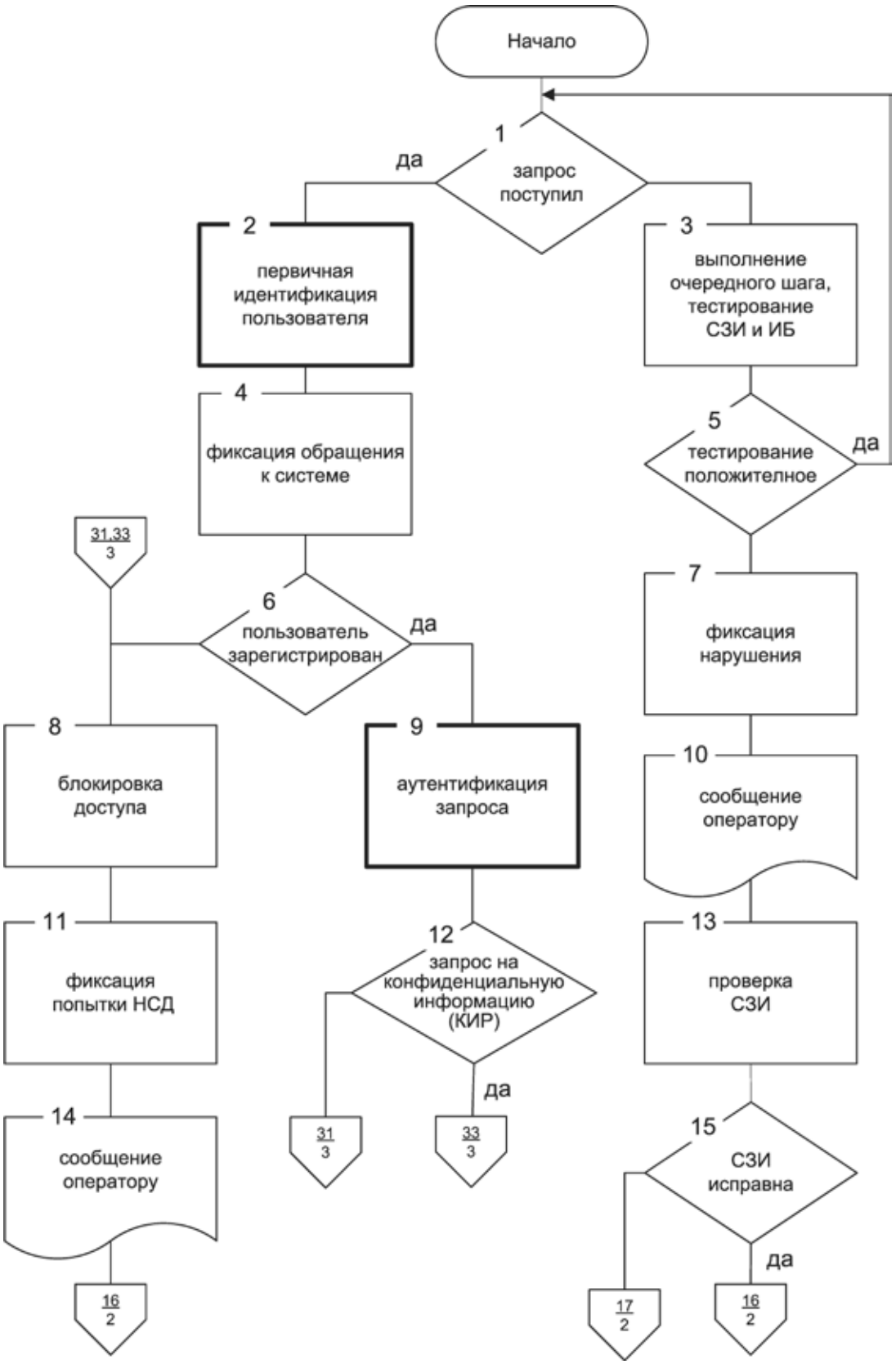

Рис. 1. Алгоритм функционирования СЗИ от НСД к АСП (начало)

называемая вторичная идентификация пользователя. Информация на внешних устройствах памяти должна храниться в закрытом виде. В таком же виде она должна передаваться по сети. Завершение обработки запроса должно сопровождаться не просто освобождением участков запоминающих устройств, то есть стиранием признака занятости, но и уничтожением остаточной информации в этих участках.

Алгоритм функционирования СЗИ от НСД, реализующий указанный перечень функций с учетом введенных допущений, приведен на рисунках 1 - 3.

Функционирование СЗИ от НСД начинается

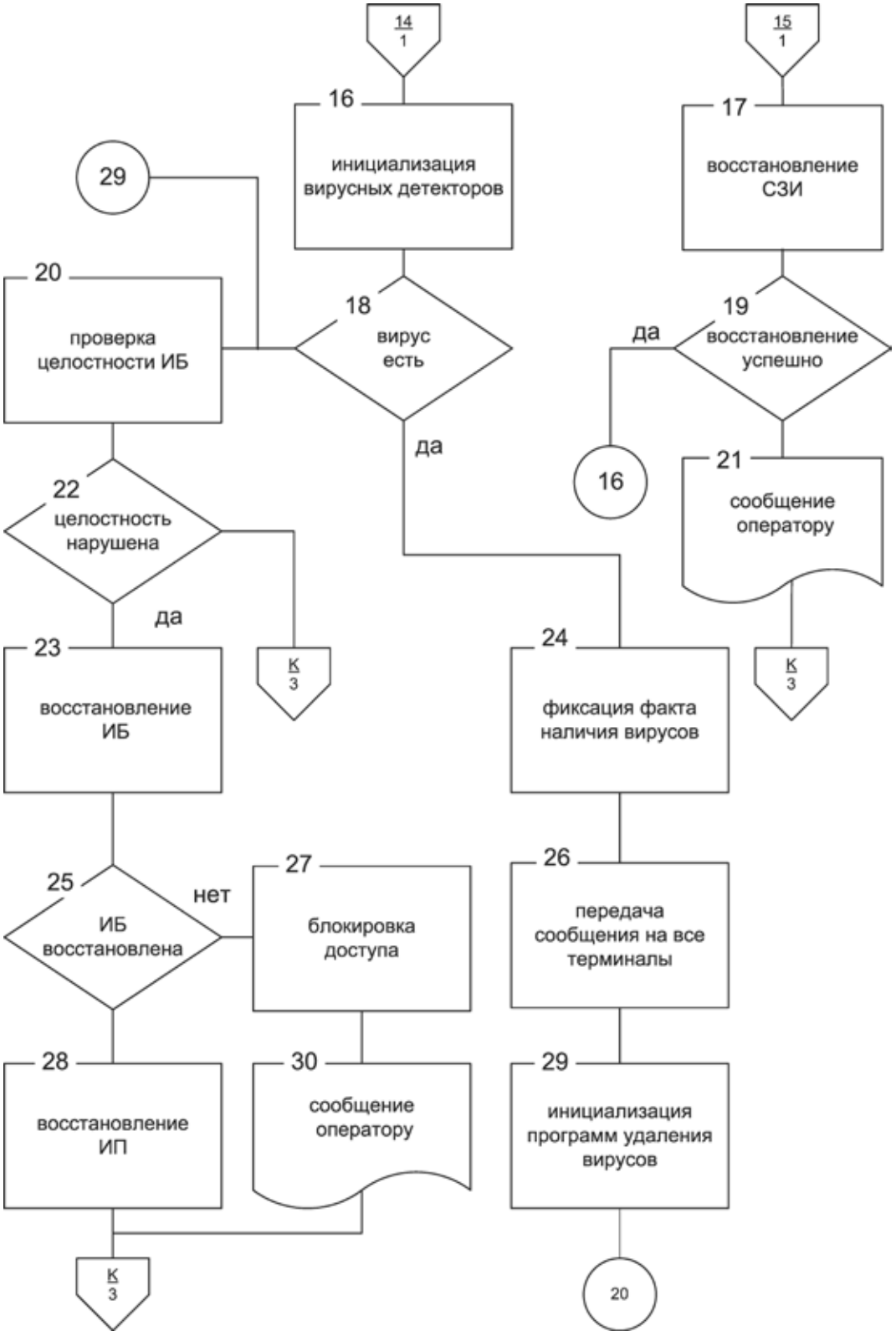

Рис. 2. Алгоритм функционирования СЗИ от НСД к АСП (продолжение)

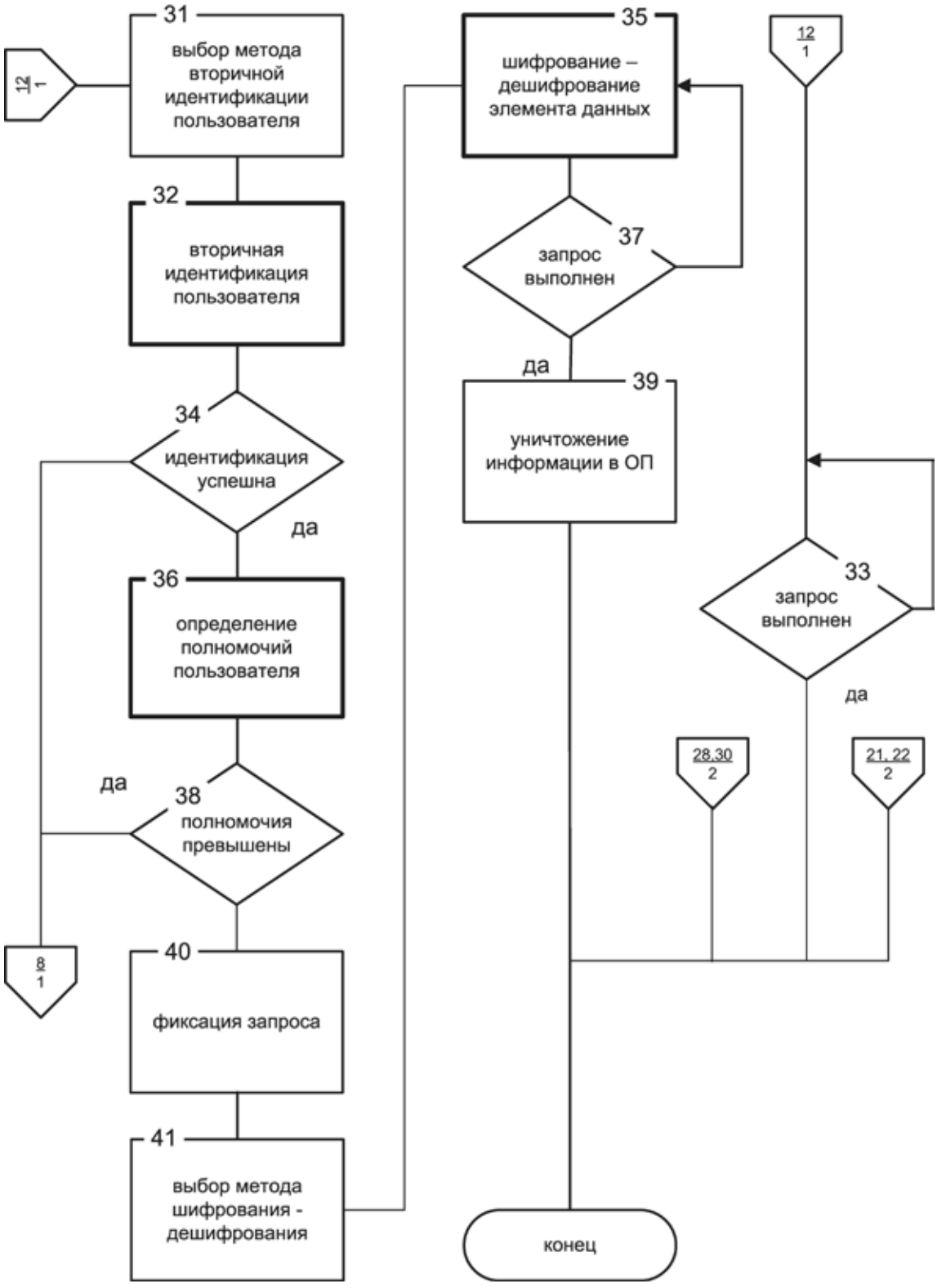

Рис. 3. Алгоритм функционирования СЗИ от НСД к АСП (окончание)

проверкой очередей запросов на решение задач в АСП (блок 1). В случае пустой очереди СЗИ от НСД инициирует в соответствии с принятыми допущениями самоконтроль, выполняемый встроенными тестовыми средствами (блок 3). Выполнение операций самоконтроля осуществляется в течение некоторого времени, после которого в случае нормального результата тестирования (блок 5) вновь проверяется наличие запроса на решение задач в АСП (блок 1).

Подобный механизм синхронизации действий системы защиты по самотестированию и отслеживанию состояния входной очереди запросов на информационно-вычислительную услугу в АСП функционирует по так называемому расписанию. Альтернативой такому решению мо-

жет служить синхронизация, выполняемая средствами штатной системы прерывания сервера, составляющей информационно-вычислительную основу АСП. Условием успешного функционирования альтернативного способа является, безусловно, меньший приоритет тестовых программ по отношению к любым прикладным.

Замкнутая траектория информационно-вычислительного процесса, проходящая через блоки 1, 3 и 5, образует цикл ожидания появления запроса на обработку данных.

В случае поступления запроса тестовый контроль прекращается, и начинают выполняться действия, связанные с первичной идентификацией пользователя (блок 2), сущность которых сводится к проверке факта регистрации субъекта. Независимо от успеха этой проверки осуществляется фиксация обращения (блок 4) в журнале регистрации.

Дальнейшее развитие процесса определяется результатом проверки регистрации пользователя (блок 6).

В случае, когда результат проверки положителен, то есть к АСП обращается законный пользователь, выполняется аутентификация запроса (блок 9) и выясняется степень конфиденциальности запрашиваемой информации (блок 12) с точностью до двух выделенных выше групп.

Принадлежность информации к первой группе прекращает вызов функций СЗИ от НСД. Последней остается лишь отслеживать момент завершения обслуживания запроса операционной системой путем организации цикла ожидания (блок 33).

В полной мере защитные свойства рассматриваемой СЗИ от НСД проявляются по отношению к информации, являющейся «закрытой». В соответствии с уровнем доступа к информации выбирается метод вторичной идентификации (блок 31), реализующий проверку подлинности субъектов, например, по биометрическим параметрам (блок 32).

Успешный исход вторичной идентификации субъекта приводит к выяснению его полномочий (блоки 36, 38), чем и завершается определение законности обращения. Если субъект действует в пределах отведенных ему прав, сгенерированный им запрос фиксируется в специальном журнале (блок 40).

Поскольку всякий пользовательский запрос связан с обработкой данных, хранимых в общей информационной базе (ИБ), то из СЗИ от НСД согласно уровню «закрытости» запрашиваемых данных и атрибутам субъекта выбирается метод криптозащиты и ключевая информация (блок 41). Только после этого запрос получает собственно доступ к данным.

Последнее выражается в инициировании циклического процесса, один этап которого состоит в шифровании-дешифровании очередного элемента данных (блок 35) в зависимости от типа операции обращения к внешним запоминающим устройствам, а другой - в отслеживании факта завершения процесса обработки запроса (блок 37). Цикл продолжается до тех пор, пока все элементы данных не будут обработаны на предмет криптозащиты. Обработка последнего элемента соответствует завершению обработки всего запроса и сопровождается стиранием остаточной информации в выделенной области памяти (блок 39).

Рассматриваемая траектория алгоритма функционирования СЗИ от НСД является основой, определяющей сущность защиты данных, и соответствует так называемым легитимным запросам и бессбойной работе системы. Оставшаяся часть алгоритма связана с обработкой нештатных ситуаций, вызванных либо незаконностью действий субъектов, либо появлением ошибок в работе.

Первая нештатная ситуация порождается попыткой обращения к АСП незарегистрированного пользователя (блок 6). В этом случае СЗИ немедленно блокирует доступ (блок 8) такого пользователя, фиксирует попытку НСД в специальном журнале нарушений (блок 11) и формирует тревожное сообщение должностному лицу, отвечающему за безопасность информации (блок 14).

Однако на этом обработка рассматриваемой ситуации не заканчивается. Учитывая, что ей предшествует первичная идентификация пользователя, выполняемая программными методами, СЗИ от НСД выполняет действия, направленные на выявление и устранение возможных последствий предпринятой попытки доступа. Эти действия сводятся в основном к актуализации антивирусных функций (блок 16). И если вирусы обнаружены (блок 18), то на сетевые устройства отображения и документирования данных передаются тревожные сообщения (блок 26), после чего выполняются процедуры удаления выявленных вирусов (блок 29).

Независимо от факта обнаружения вирусов осуществляется проверка целостности информационной базы (блок 20) в полном объеме. При необходимости включаются функции восстановления (блок 23), успешная реализация которых (блок 25) влечет восстановление информационного процесса, прерванного в результате возникновения нештатной ситуации.

Невозможность восстановления информационной базы приводит к блокировке любого доступа, в том числе и легитимного (блок 27). Иными словами, вычислительный процесс по обслуживанию заявок на решение задач управления прерывается.

Дальнейшие действия выходят за рамки возможностей СЗИ от НСД по автоматическому устранению последствий возникновения нештатной ситуации и определяются персоналом, обслуживающим АСП. Инициирует эти действия

СЗИ от НСД путем формирования сообщения оператору (блок 30).

Вторая нештатная ситуация возникает, когда зарегистрированный пользователь АСП пытается выдать себя за другого, также зарегистрированного пользователя (блок 34), либо превысить свои, заранее оговоренные, полномочия (блок 38). Эта ситуация подвергается анализу в том же объеме, что и попытка войти в АСП незарегистрированному пользователю (блок 8).

Наконец, третья ситуация, требующая прерывания информационно-вычислительного процесса в АСП, напрямую не связана с преднамеренными попытками несанкционированного доступа, а является следствием возникновения ошибок в СЗИ от НСД (блок 5), которая является объектом анализа в этом случае. Проверка системы (блок 13) осуществляется лицом, ответственным за безопасность информации, после фиксации в журнале нарушений (блок 7) и выдачи сообщения на устройства отображения и документирования (блок 10).

Наличие устранимой ошибки позволяет квалифицировать ее как сбой и сделать вывод об исправности СЗИ от НСД (блок 15). В этом случае перед переводом системы в штатный режим выполняется тестирование информационной базы на наличие вирусов (блок 16) в том же объеме, как это было описано для первой ситуации. Объясняется такая предусмотрительность возможностью возникновения ошибки в результате активизации вирусов.

В случае, когда ошибка является результатом отказа системы защиты, принимаются усилия по ее восстановлению (блок 17). Удачное решение этой задачи влечет проверку целостности информационной базы (блок 16) по изложенному выше алгоритму. Более серьезный отказ требует вмешательства оператора АСП, что инициируется выдачей ему сообщения (блок 21). При этом информационно-вычислительный процесс прерывается на неопределенно длительное время.

Представленный алгоритм функционирования реализует все вышеуказанные основные функции с учетом введенных допущений, охватывает все значимые ситуации как штатные, так и аварийные, и в этой связи может быть положен в основу математической модели СЗИ от НСД.

При формировании математической модели все множество значимых факторов условно разделяется на непересекающиеся подмножества: одно из них служит исходными данными для построения целевой функции, другое вводится в состав ограничений. Упомянутые подходы являются альтернативными и инверсными.

Выбор того или иного подхода определяется приоритетом потребительских свойств СЗИ от НСД. Применительно к модели СЗИ от НСД к критическим информационным ресурсам в АСП требования к защищенности информации, которые, безусловно, должны быть выполнены, необходимо отнести к ограничениям, а целевую функцию необходимо формировать на основе затратных показателей.

В случае оптимизации подобной модели СЗИ от НСД достигается минимальная цена заданного уровня защищенности информации в АСП. В противном случае (альтернативный подход) достигается максимально возможная в заданных условиях степень защищенности КИР.

Возможны комбинации подходов по типу «достижение максимальной защищенности при соблюдении ограничения на общую стоимость затрат».

Среди всех показателей, отражающих издержки на СЗИ от НСД, основными являются T – время и S – стоимость обработки одного запроса на информационно-вычислительный ресурс АСП.

Первый показатель приобретает значимость в связи с тем, что СЗИ от НСД реализует свои основные функции, как правило, за счет информационно-вычислительных ресурсов АСП. Второй показатель соответствует финансовым затратам на приобретение и поддержание в работоспособном состоянии элементов СЗИ от НСД.

В случае оптимизации оба показателя, на основе которых должна быть сформирована целевая функция, подлежат минимизации.

Этот факт позволяет выполнить свертку обоих показателей методом мультипликативного взвешивания.

Тогда целевую функцию можно свести к виду

$$C = T^{k1} S^{k2}, \quad (1)$$

где $k1 + k2 = 1$ - весовые коэффициенты или коэффициенты неравнозначности, определяющие различие важности показателей *T* и *S*.

Оба затратных показателя, входящих в целевую функцию, должны определяться дифференцированно для каждого шага функционирования СЗИ от НСД согласно алгоритму. Этот алгоритм содержит целый ряд пересекающихся траекторий его выполнения, зависящих от условий работы системы. Выбор той или иной траектории зависит от множества факторов и может быть описан вероятностным образом. Следовательно, модель СЗИ от НСД также должна быть построена как вероятностная. Последнее, в свою очередь, означает, что целевая функция должна представляться аддитивной взвесью ценовых функций каждого элемента блок-схемы алгоритма (в качестве весовых коэффициентов могут использоваться вероятности выполнения отдельных шагов).

То есть:

$$C = \sum_i P_i \cdot C_i , \qquad \text{где} \quad C_i = T_i^{k1} \cdot S_i^{k2}. \qquad (2)$$

Здесь индекс i соответствует номеру элемента алгоритма.

Иными словами, целевая функция должна выражать математическое ожидание ценовых функций всех элементов алгоритма.

Тогда с учетом нумерации блоков алгоритма, принятой на рисунках 1 - 3, можно записать:

$$C = C_1 + P_{1,2} \cdot C_{2,end} + (1 - P_{1,2}) \cdot C_{3,end} , \qquad (3)$$

где C_1 - цена выполнения проверки поступления запроса в АСП (цена блока 1);

$C_{2,end}$ и $C_{3,end}$ - цена работы СЗИ от НСД по траекториям от 2-го и 3-го блоков соответственно до конечного блока алгоритма;

$P_{1,2}$ - вероятность перехода от 1 ко 2 блоку алгоритма.

В свою очередь,

$$C_{3,end} = C_3 + C_5 + P_{5,7} \cdot C_{7,end} + (1 - P_{5,7}) \cdot C . \qquad (4)$$

Подстановка $C_{3,end}$ дает

$$\begin{aligned} C = {} & C_1 + P_{1,2} \cdot C_{2,end} + \\ & + (1 - P_{1,2})(C_3 + C_5 + P_{5,7} \cdot C_{7,end}) + \\ & + (1 - P_{1,2})(1 - P_{5,7}) \cdot C. \end{aligned} \qquad (5)$$

Полученное выражение представляет собой уравнение с одним неизвестным.

Решая его относительно C, нетрудно получить:

$$C = \frac{C_1 + P_{1,2} \cdot C_{2,end} + (1 - P_{1,2})(C_3 + C_5 + P_{5,7} \cdot C_{7,end})}{1 - (1 - P_{1,2}) \cdot (1 - P_{5,7})} . \qquad (6)$$

В свою очередь, переменная $C_{2,end}$ может быть представлена в виде:

$$\begin{aligned} C_{2,k} = {} & C_2 + C_4 + C_6 + P_{6,8} \cdot C_{8,end} + \\ & + (1 - P_{6,8}) \cdot C_{9,end} . \end{aligned} \qquad (7)$$

Следующие шаги построения целевой функции C должны быть связаны с представлением вновь вводимых функций $C_{i,end}$ (где i - номера блоков, следующих за блоками условного перехода) через другие частные ценовые функции.

Таким образом, общее выражение для C получается многоступенчатым. Каждая ступень соответствует продвижению к конечному блоку алгоритма по выбранной траектории на "расстояние" до следующего блока условного перехода. Если каждой ступени поставить в соответствие одну итерацию, то процедуру формирования целевой функции можно рассматривать как итерационную. Число итераций определяется возможным числом ветвлений алгоритма функционирования СЗИ от НСД.

Нетрудно показать, что итоговое выражение для целевой функции имеет вид:

$$\begin{aligned} C = {} & \frac{1}{1 - P_{1,3}P_{5,1}} (T_1^{k1} S_1^{k1} + P_{1,2} C_{2,k} + \\ & + P_{1,3} (T_3^{k1} S_3^{k1} + T_5^{k1} S_5^{k1} + P_{5,7} C_{7,end})), \end{aligned} \qquad (8)$$

где

$$\begin{aligned} C_{2,k} = {} & T_2^{k1} S_2^{k1} + T_4^{k1} S_4^{k1} + T_6^{k1} S_6^{k1} + \\ & + P_{6,8} C_{8,end} + P_{6,9} C_{9,end}; \\ C_{7,k} = {} & T_7^{k1} S_7^{k1} + T_{10}^{k1} S_{10}^{k1} + T_{13}^{k1} S_{13}^{k1} + T_{15}^{k1} S_{15}^{k1} + \\ & + P_{15,16} C_{16,end} + P_{15,17} C_{17,end}; \end{aligned}$$

$$\begin{aligned} C_{8,k} = {} & T_8^{k1} S_8^{k1} + T_{11}^{k1} S_{11}^{k1} + T_{14}^{k1} S_{14}^{k1} + T_{16}^{k1} S_{16}^{k1} + \\ & + T_{18}^{k1} S_{18}^{k1} + P_{18,20} C_{20,end} + P_{18,24} C_{24,end}; \\ C_{9,k} = {} & T_9^{k1} S_9^{k1} + T_{12}^{k1} S_{12}^{k1} + P_{12,31} C_{31,end} + P_{12,33} C_{33,end}; \\ C_{16,k} = {} & T_{16}^{k1} S_{16}^{k1} + T_{18}^{k1} S_{18}^{k1} + P_{18,20} C_{20,end} + P_{18,24} C_{24,end}; \\ C_{17,k} = {} & T_{17}^{k1} S_{17}^{k1} + T_{19}^{k1} S_{19}^{k1} + P_{19,16} C_{16,end} + \\ & + P_{19,21} \left(T_{21}^{k1} S_{21}^{k1} + T_{end}^{k1} S_{end}^{k1} \right); \\ C_{20,k} = {} & T_{20}^{k1} S_{20}^{k1} + T_{22}^{k1} S_{22}^{k1} + \\ & + P_{22,end} T_{end}^{k1} S_{end}^{k1} + P_{22,23} C_{23,end}; \\ C_{24,k} = {} & T_{24}^{k1} S_{24}^{k1} + T_{26}^{k1} S_{26}^{k1} + T_{29}^{k1} S_{29}^{k1} + C_{20,end}; \\ C_{31,k} = {} & T_{31}^{k1} S_{31}^{k1} + T_{32}^{k1} S_{32}^{k1} + T_{34}^{k1} S_{34}^{k1} + \\ & + P_{34,8} C_{8,end} + P_{34,36} C_{36,end}; \\ C_{12,k} = {} & T_{12}^{n} C_{12} + T_{33}^{n} C_{33} + P_{33,33} C_{33,end} + P_{33,k} T_k^n C_{end}; \\ C_{23,k} = {} & T_{23}^{k1} S_{23}^{k1} + T_{25}^{k1} S_{25}^{k1} + P_{25,27} C_{27,end} + \\ & + P_{25,28} \left(T_{28}^{k1} S_{28}^{k1} + T_{end}^{k1} S_{end}^{k1} \right); \\ C_{36,k} = {} & T_{36}^{k1} S_{36}^{k1} + T_{38}^{k1} S_{38}^{k1} + P_{38,8} F_{8,end} + P_{38,40} C_{40,end}; \\ C_{27,k} = {} & T_{27}^{k1} S_{27}^{k1} + T_{30}^{k1} S_{30}^{k1} + T_{end}^{k1} S_{end}^{k1}; \\ C_{40,k} = {} & T_{40}^{k1} S_{40}^{k1} + T_{41}^{k1} S_{41}^{k1} + C_{35,end}; \\ C_{35,k} = {} & T_{35}^{k1} S_{35}^{k1} + T_{37}^{k1} S_{37}^{k1} + P_{37,35} C_{35,end} + \\ & + P_{37,39} \left(T_{39}^{k1} S_{39}^{k1} + T_{end}^{k1} S_{end}^{k1} \right). \end{aligned}$$

Здесь

$C_{i,end}$ - ценовая функция обработки запроса на информационно-вычислительный ресурс на участке от *i*-го блока алгоритма до конечного;

T_i - относительное время обработки запроса в *i*-ом блоке;

S_i - относительная стоимость обработки запроса в *i*-ом блоке;

$P_{i,j}$ - вероятность перехода от *i*-го блока к *j*-му.

Второй элемент модели - ограничения - необходимо формировать в виде неравенств типа:

$$W^{Д}_{НСД_n} \le W^{T}_{НСД_n}, \quad n = \overline{1, N} , \qquad (9)$$

где $W^{Д}_{НСД_n}$ - действительная, то есть обеспечиваемая СЗИ вероятность НСД к КИР *n*-ой категории секретности;

$W^{T}_{НСД_n}$ - требуемая вероятность НСД к КИР той же категории.

Согласно представленному алгоритму функционирования СЗИ от НСД к АСП значение вероятности НСД определяется пятью процедурами, выполняемыми СЗИ: шифрованием-дешифрованием данных (блок 35); первичной идентификацией пользователей (блок 2); аутентификацией запросов (блок 9); проверкой полномочий пользователей (блок 36); вторичной идентификацией пользователей (блок 32).

Учитывая, что перечисленные процедуры независимы, можно записать:

$$W^{Д}_{НСД_n} = W_{2nl} \cdot W_{9nm} \cdot W_{32ne} \cdot W_{35ng} \cdot W_{36ny} \le W^{T}_{НСД_n},$$
$$l = \overline{1,L}, \quad m = \overline{1,M}, \quad e = \overline{1,E}, \qquad (10)$$
$$g = \overline{1,G}, \quad y = \overline{1,Y},$$

где N - количество категорий секретности;

L - количество методов первичной идентификации;

M - количество методов аутентификации;

E - количество методов вторичной идентификации;

G - количество методов шифрования/дешифрования КИР;

Y - количество методов проверки полномочий.

Таким образом, сформирована целевая функция и ограничения, которые в совокупности можно рассматривать как математическую модель СЗИ от НСД к критическим информационным ресурсам при проектировании АСБУ кораблей ВМФ в автоматизированной среде.

СПИСОК ЛИТЕРАТУРЫ

1. Осипов В.Ю. Оценка защищенности информационно-вычислительных ресурсов от НСД // Приборы и системы управления. - 1996. - № 7.— С. 16-19.

2. Андриенко А.А., Максимов Р.В. Защита информации. - Ч. 1, 2.— СПб.: ВУС, 2004.

3. Буйневич М. В., Кляхин В. Н. Сущность и содержание концепции защиты информации при проведении научных исследований// Безопасность информации. Компьютерные технологии. - 2003. - № 3.