УДК 681.3

ИННОВАЦИОННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ: СТРУКТУРНАЯ МОДЕЛЬ КОНТРОЛЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИИ

С.В. Скрыль, С.В. Белокуров, О.В. Багринцева, С.Н. Волкова

В статье показаны этапы разработки методического обеспечения комплексной оценки качества функционирования средств защиты от несанкционированного доступа, и на её основе организация процессов оптимального управления доступом пользователей к информации в условиях информационных проектов интеграции

Ключевые слова: пользователь,безопасность, интегрированные системы

Определение основных этапов разработки методического обеспечения (МО) задач исследования осуществляется на основе анализа задач и этапов автоматизированного управления качеством средств защиты информации от несанкционированного доступа (СЗИ НСД). Задача оптимального управления доступом пользователей к информации в интегрированных системах безопасности (ИСБ) осуществляется на основе комплексной оценки качества функционирования СЗИ НСД.

Структурная модель управления контролем доступа пользователей к информации в ИСБ представлена на (рис. 1). В модифицированной системе защиты информации от несанкционированного доступа (МСЗИ НСД) (рис. 1) в качестве подсистемы управления доступом используется подсистема многоуровневого управления доступом пользователей.

Для поддержки принятия администратором защиты информации (ЗИ), лица принимающего решение (ЛПР), решений по оптимальному управлению контролем доступа пользователей к информации в ИСБ с помощью управляемых параметров предлагается использовать новую подсистему – подсистему автоматизированного контроля доступа пользователей в ИСБ, представленную на (рис. 1).

Исходными данными для нее являются:

1) статистические данные о вероятностно-временных характеристиках (ВВХ) реализации функций ЗИ при выполнении СЗИ НСД своих сервисных задач в ИСБ. Эти данные предоставляются подсистемой регистрации и учета;

2) параметры, задающие требования к управлению качеством функционирования СЗИ НСД как в плане обеспечения ЗИ от НСД, так и в плане обеспечения функционирования ИСБ по прямому назначению.

Эти данные задаются администратором ЗИ в соответствии с разделом «Требования к подсистеме ЗИ от НСД» эксплуатационной документации на ИСБ.

Подсистема автоматизированного контроля доступа пользователей в ИСБ (рис. 1) включает в свой состав подсистему контроля качества функционирования СЗИ НСД, подсистему принятия решений, подсистему управляющих воздействий.

Подсистема контроля качества функционирования СЗИ НСД осуществляет оценку количественного критерия качества функционирования СЗИ НСД, на основе данных о выполнении СЗИ НСД своих сервисных задач в ИСБ.

Эти данные предоставляются подсистемой регистрации и учета. Оценка качества функционирования СЗИ НСД производится в данном случае с целью реализации функции обратной связи процесса управления качеством функционирования СЗИ НСД ИСБ.

Подсистемой принятия решений реализуется ЗПР по оптимальному управлению качеством функционирования СЗИ НСД, являющаяся ключевой при организационно-технологическом управлении контролем доступа пользователей в ИСБ.

Принятие решения осуществляется на основе комплексной оценки качества функционирования СЗИ НСД для обеспечения и поддержания разумного

Скрыль Сергей Васильевич – ВИ ФСИН России, д-р техн. наук, профессор, e-mail: bsvlabs@mail.ru
Белокуров Сергей Владимирович – ВИ ФСИН России, д-р техн. наук, профессор, e-mail: bsvlabs@mail.ru
Багринцева Оксана Владимировна – ВИ МВД России, адъюнкт, e-mail:ganych-oksana@rambler.ru
Волкова Светлана Николаевна – ВИ МВД России, адъюнкт, e-mail: dgersi.87@mail.ru

компромисса между уровнем защищенности информации в ИСБ и эффективностью функционирования ИСБ по прямому назначению.

Комплексная оценка качества функционирования СЗИ НСД как объекта управления производится по векторному критерию, компонентами которого являются частные критерии качества функционирования СЗИ НСД.

В результате управленческого решения выбирается такой набор значений управляемых параметров функционирования СЗИ НСД, который обеспечивает максимальное значение интегрального критерия качества функционирования СЗИ НСД как объекта управления контролем доступа пользователей

.

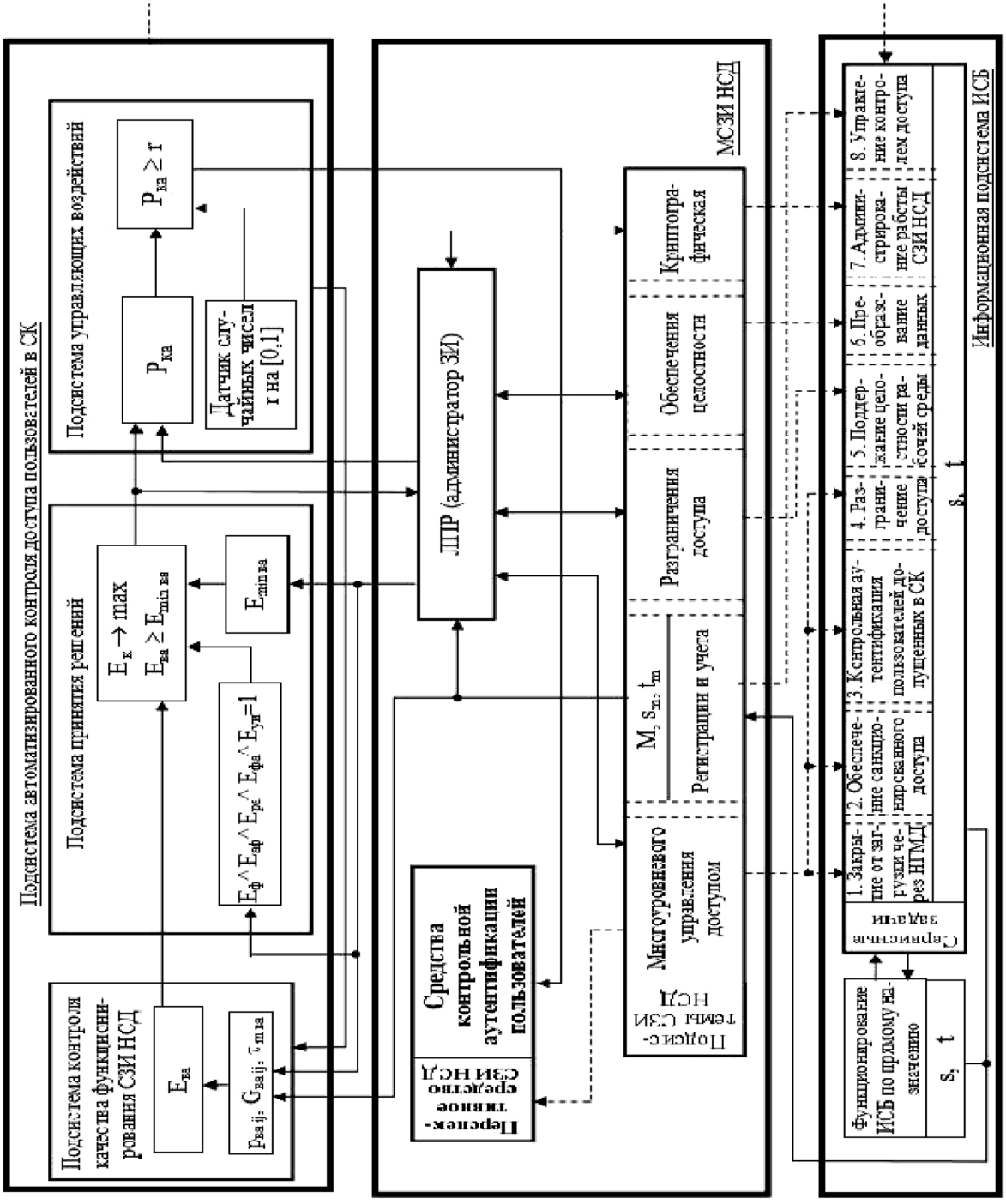

Рис. 1. Структурная модель управления контролем доступа пользователей к информации в ИСБ

Подсистема управляющих воздействий формирует управляющее воздействие на СЗИ НСД в соответствии с принятым решением (набором значений управляемых параметров). При этом выбранный набор значений управляемых параметров используется подсистемой управляющих воздействий для определения конкретного момента запуска программы подсистемы управления доступом, но так, чтобы пользователи не могли по возможности прогнозировать этот момент времени.

Таким образом, задачу принятия решения при организационно-технологическом управлении качеством функционирования СЗИ НСД ИСБ можно формализовать как задачу безусловной оптимизации следующим образом. Требуется выбрать такую альтернативу (набор значений управляемых параметров функционирования СЗИ НСД) $a \in A$ из множества альтернатив (всех возможных таких наборов), чтобы комплексный критерий качества функционирования СЗИ НСД как объекта управления $E_к$ достигал на этой альтернативе своего максимального значения:

$$E_к(a) \to \max. \qquad (1)$$

В результате анализа задач и этапов управления контролем доступа пользователей в ИСБ, на основе комплексной оценки её качества функционирования, разработана структурная схема разработки МО автоматизированного контроля доступа пользователей к информации в ИСБ, представленная на рис. 2.

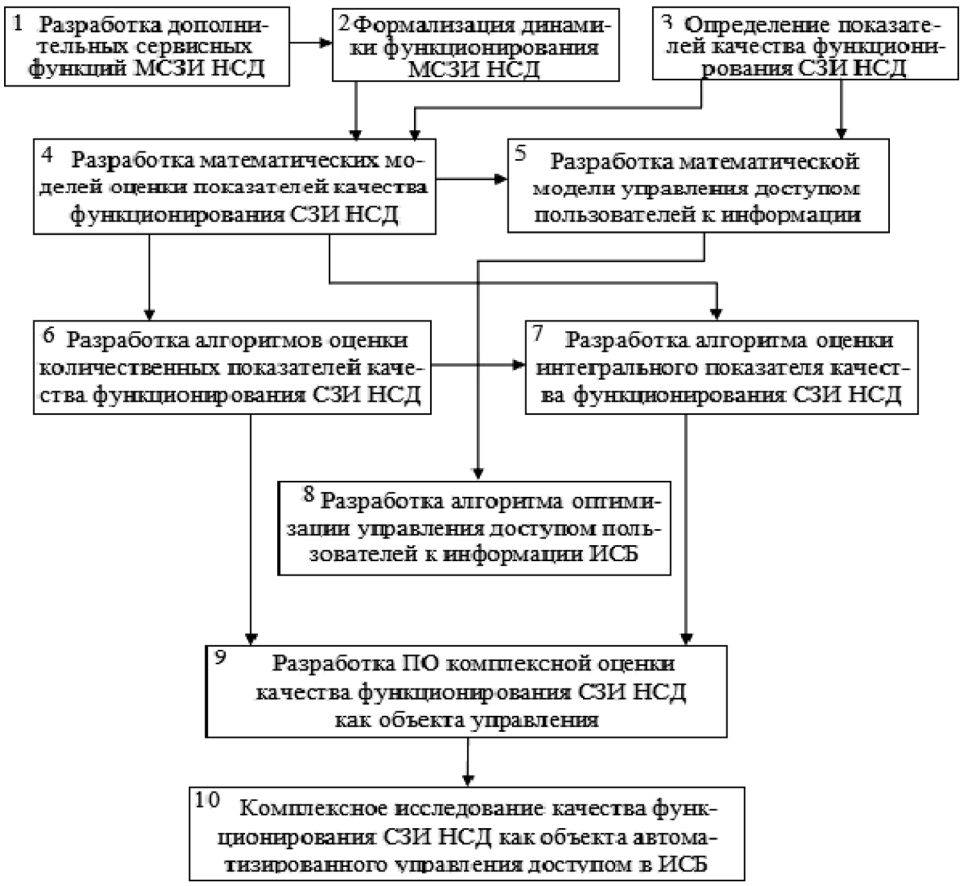

Рис. 2. Структурная схема разработки МО

Для повышения защищенности ИСБ необходимо разработать процедуру многоуровневого управления доступом пользователей для подсистемы управления доступом МСЗИ НСД (задача 1 на рис. 2). С учетом разработанных перспективных функций СЗИ НСД необходимо создать математическую модель динамики функционирования МСЗИ НСД в ИСБ как системы массового обслуживания (задача 2 на рис. 2) для моделирования количественного критерия качества

функционирования СЗИ НСД. Для МО комплексной оценки качества функционирования СЗИ НСД как объекта управления контролем доступа необходимо разработать систему критериев качества функционирования СЗИ НСД, автоматизированного контроля доступа пользователей к информации в ИСБ математические модели и алгоритмы для оценки этих критериев и способ оценки интегрального критерия по известным частным (задачи 3, 4, 6, 7 на рис. 2).

На основе комплексной оценки качества функционирования СЗИ НСД как объекта управления контролем доступа пользователей необходимо предложить способы и алгоритмы оптимального управления качеством СЗИ НСД в ИСБ с помощью управляемых параметров средств ЗИ (задачи 5, 8 на рис. 2) для решения проблемы МО автоматизированного управления контролем доступа пользователей в СК.

Для апробации МО автоматизированного контроля доступа пользователей в ИСБ необходимо разработать ПО комплексной оценки качества функционирования МСЗИ НСД как объектов управления (задача 9 на рис. 2) и провести комплексное исследование качества её функционирования (задача 10 на рис. 2).

Одной из основных задач СЗИ НСД ИСБ является управление доступом пользователей к информационным ресурсам ИСБ с помощью процедур идентификации и аутентификации пользователей, с целью предотвращения доступа злоумышленника к конфиденциальной информации [1]. Проведенные исследования качества функционирования СЗИ НСД в ИСБ [1] показали высокую значимость функции управления доступом в решении проблемы ЗИ ИСБ, особенно в условиях возрастания угроз информационной безопасности (ИБ). Управление доступом к информации должно обеспечивать и в самых неблагоприятных условиях функционирования ИСБ, в смысле угроз ИБ, малую вероятность проникновения злоумышленника в систему. Тогда реализация других функций СЗИ НСД позволит достигнуть еще более высокого уровня защищенности информации, не нарушая требуемой эффективности функционирования ИСБ по прямому назначению.

Значимость этих процедур для решения проблемы ЗИ ИСБ подтверждается результатами исследований, проведенных специалистами аналитической компании IDC, выявившими существующую мировую тенденцию приоритетного развития средств аутентификации в секторе программных продуктов ИБ. На основе анализа результатов проведенных ранее исследований качества функционирования СЗИ НСД, а также учитывая существующую мировую тенденцию приоритетного развития средств аутентификации в секторе программных продуктов ИБ, можно сделать вывод об актуальности задачи усиления подсистемы управления доступом в перспективных СЗИ НСД.

Согласно руководящему документу ГТК РФ по ЗИ от НСД [1]: идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов; аутентификация (подтверждение подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора.

Процедуры идентификации и аутентификации пользователей проводятся практически во всех АС, оснащенных средствами защиты, для опознания пользователя как субъекта доступа с целью реализации правила разграничения доступа (ПРД). Сложность процедуры и средств идентификации и аутентификации пользователей, которые целесообразно применять в автоматизированных системах (АС), должна зависеть от класса защищенности АС от НСД к информации. Классификация АС по защищенности от НСД к информации и требования по ЗИ, предъявляемые к АС и в частности к средствам идентификации и аутентификации, приводятся в [2]. Представленные в этом источнике классы защищенности АС от НСД к информации подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа включает АС, в которых пользователи допущены ко всей информации АС (имеют одинаковые полномочия), размещенной на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разного уровня конфиденциальности. Пользователи имеют различные полномочия по доступу к информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС [2].

Типовой алгоритм идентификации и аутентификации пользователей, приведенный в [1], представляет собой последовательное выполнение процедур идентификации и аутентификации пользователей СЗИ НСД при доступе к конфиденциальной информации ИСБ. Пользователь при входе в систему идентифицирует себя с помощью идентификатора. Для этого у пользователя запрашивается учетный номер и (или) идентификатор, которые сравниваются с данными списка пользователей, занесенного в память ИСБ. В случае отрицательного результата сравнения обращающемуся отказывается в доступе в систему, о чем он оповещается, а также регистрируется неудовлетворительная попытка идентификации и при превышении количества попыток заданного числа блокируется терминал и оповещается администратор службы безопасности о НСД к информации. Учитывая, что идентификатор пользователя представляет собой неизменную и достаточно доступную информацию, после идентификации проводят аутентификацию, с целью проверки, является ли проверяемый субъект на самом деле тем, за кого себя выдает. Для этого при положительном исходе идентификации пользователя запускается процедура его аутентификации, в процессе которой запрашивается дополнительная информация (пароль, биометрические данные и т. д.) от пользователя. По результатам сравнения полученных данных и хранящихся в памяти ИСБ принимается решение о допуске пользователя в систему. Причем, реакция системы на отрицательный результат сравнения аналогичная реакции при процедуре идентификации. Сложность процедуры и средств идентификации и аутентификации пользователей, которые целесообразно применять в ИСБ, должны зависеть от конфиденциальности (ценности) защищаемой информации.

Рассмотренные процедуры управления доступом в общем случае обеспечивают санкционированный доступ пользователей в ИСБ, но все же существует немалая вероятность использования злоумышленником параметров аутентификации санкционированных пользователей при доступе в систему, замещения злоумышленником санкционированного пользователя в процессе его работы в ИСБ и другие способы НСД злоумышленника к информационным ресурсам ИСБ. Все это определяет актуальность внедрения в подсистему управления доступом процедуры проверки подлинности пользователей в процессе их работы в системе (контрольная аутентификация).

Для повышения защищенности ИСБ, учитывая вышесказанное, предлагается использовать подсистему многоуровневого управления доступом в МСЗИ НСД ИСБ выполняющую, кроме стандартной процедуры аутентификации, процедуры контрольной аутентификации пользователей к информации ИСБ. Использование подсистемы многоуровневого управления доступом особенно важно для многопользовательских ИСБ, относящихся к первой группе классов защищенности от НСД, обрабатывающих информацию большого набора уровней конфиденциальности и имеющих широкую

номенклатуру пользователей с различными полномочиями по доступу к информации ИСБ.

Процедура контрольной аутентификации выполняется при обращении к информационному ресурсу после доступа пользователей в систему. Для аутентификации пользователей целесообразно применять разовые пароли, биометрические средства и методы “запрос-ответ”, “рукопожатие” или их комбинацию. Проверка подлинности пользователя по методам “запрос-ответ” или “рукопожатие” осуществляется по результатам соответственно ответов на выбранные СЗИ НСД вопросы, хранящиеся в памяти, или корректной обработки заданного алгоритма [3]. При реализации процедуры контрольной аутентификации можно использовать метод разделенных привилегий, обеспечивающий доступ к ресурсу при одновременной аутентификации всех членов некоторой группы (например, пользователь, представитель службы безопасности и администратор системы). Совокупность процедур типовой и контрольной аутентификации пользователей, выполняемых при обращении к информационному ресурсу ИСБ, обеспечивает высокий уровень защиты системы от НСД.

Таким образом, разработан многоуровневый алгоритм управления доступом пользователей к информационным ресурсам ИСБ. С целью повышения защищенности ИСБ, особо критичной к проблеме ЗИ, предлагается использовать в подсистеме управления доступом МСЗИ НСД, вместо типового алгоритма, разработанный многоуровневый алгоритм управления доступом пользователей к информации.

Литература

1. Основы информационной безопасности: учебник для высших учебных заведений МВД России / под ред. В.А. Минаева и С.В. Скрыля. - Воронеж: Воронежский институт МВД России, 2001. - 464 с.

2. Методы и средства автоматизированного управления подсистемой контроля целостности в системах защиты информации / Е.А. Рогозин, А.С. Дубровин, В.И. Сумин и др. // Монография. – Воронеж: Воронеж. гос. техн. ун-т, 2003. – 165 с.

3. Белокуров С.В. Особенности функционирования системы контроля и управления доступом в интегрированных системах безопасности / С.В. Белокуров, О.В. Багринцева // Проблемы обеспечения надежности и качества приборов, устройств и систем: межвуз. сб. науч. тр. Воронеж: ВГТУ, 2011. – С. 60-63.

Воронежский институт МВД России
Воронежский институт ФСИН России
Voronezh Institute of the Ministry of the Interior of Russia
Voronezh institute of the Russian Federal penitentiary service

OBJECTS AND SUBJECTS SECURITY MONITORING ON THE BASIS OF R-IDENTIFICATION TECHNOLOGY APPLICATION

S.V. Skryl`, S.V. Belokurov, O.V. Bagrintceva, S.N. Volkova

In article development stages of methodical providing a complex assessment of quality of functioning of means of protection from unauthorized access, and on its basis the organization of processes of optimum control by access of users to information in the conditions of information projects of integration are shown

Key words: the user, safety, the integrated systems