УДК 004.56 DOI: 10.26102/2310-6018/2019.26.3.018

В.С. Оладько

ФОРМАЛИЗАЦИЯ ПРОЦЕДУРЫ АУДИТА ПОДСИСТЕМЫ УПРАВЛЕНИЯ ДОСТУПОМ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации»
Москва, Россия

В статье затрагиваются актуальные на сегодняшний день проблемы и инструментарий обеспечения безопасности информации в информационных системах. Проанализированы современные тенденции нарушений информационной безопасности в 2018-2019 годах, сделан вывод об актуальности противодействия угрозам, связанным с несанкционированным доступом. Базовыми инструментами защиты информационной системы от несанкционированного доступа являются множество прав и правил управления доступом между объектами и субъектами. Поэтому для обеспечения необходимого уровня безопасности важна адекватность и логичность распределения прав доступа. Автором разработана методика и концептуальная схема проведения аудита подсистемы контроля и разграничения доступа в ИИ на основании ACL списков, состоящая из процедур инициирования аудита, сбора и анализа данных аудита. Представлено ее математическое описание в основе которого лежит подход, основанный на теории множеств. Предложенная процедура для удобства применения была автоматизирована в виде программного средства аудита подсистемы управления доступом на примере операционной системы Windows. Основным преимуществом предложенной процедуры аудита является то, что она не требует проведения сложных процедур тестирования, расчета вероятностей, привлечения и подбора экспертов и может быть использована для оценивания соответствия существующих настроек политики управления доступом в системе требованиям политики безопасности исследуемой системы.

Ключевые слова: права доступа, защита информации, операционная система, модель управления доступом, математическая модель.

Введение

В настоящее время одной из актуальных угроз информационной безопасности является угроза, связанная с кражей информации, посредством реализации целевых атак (62% в IV квартале 2018 года [1]), направленных на получение нарушителем несанкционированного доступа к информационной инфраструктуре, атакуемого объекта. По данным Positive Technologies нарушители похищают преимущественно персональные данные (30%), учетные данные (24%) и данные платежных карт (14%). Для противодействия данным угрозам и снижения рисков от последствий в рамках системы кибербезопасности [2] информационной инфраструктуры применяются подсистемы управления и разграничения доступа. Однако, как показывает практика [3 - 4], системы безопасности сами могут подвергаться воздействиям злоумышленника и становиться угрозой, особенно если они

обладают повышенными привилегиями доступа или контролируют ключевые информационные потоки. Следовательно, актуальной задачей является не только защита информационной инфраструктуры предприятия от несанкционированного доступа, аудит защищенности автоматизированных компонентов [5], но и контроль над эффективностью и состоянием безопасности самой подсистемы управления и контроля доступа.

Объектом исследования является подсистема разграничения и управления доступом пользователей информационной инфраструктуры предприятия.

Предметом исследования является уровень защищенности (безопасности) подсистемы разграничения и управления доступом пользователей.

Целью работы является разработка формализованного подхода к проведению аудита политики управления и разграничения доступа пользователей к объектам ИИ на примере операционной системы семейства Windows. Для достижения поставленной цели были решены задачи:

1. Описание этапов разработанной процедуры аудита политики управления и разграничения доступа пользователей.
2. Разработка математического описания процедуры аудита политики управления и разграничения доступа пользователей.
3. Автоматизация предложенной процедуры посредством программными с графическим пользовательским интерфейсом под ОС Windows.

Материалы и методы

В качестве основных методов исследования при выполнении работы были использованы: метод описания, системного анализа, элементы теории множества, программирование.

Ключевой целью реализации политики контроля и разграничения доступа пользователей к ресурсам информационной инфраструктуры (ИИ) является предотвращения угроз и рисков, связанных с несанкционированным доступом внешних и внутренних злоумышленников к информационным ресурсам и данным ИИ, которые представляют собой множество объектов доступа.

Исследованием вопросов, связанных с политиками управления доступом занимались такие авторы как: Семенова А.А. [6], Колегов Д.Н., Ткаченко Н.О. [7], Миронова В. Г., Шелупанов А.А. [8], 9. Куракин А.С., Костырева А.А. [9] и другие. Исходя из анализа материалов работ можно сделать вывод, что большинство направлений исследований связаны с совершенствованием функционала существующих классических моделей разграничения доступа, разработкой семантического контекста и

механизмов проекции ролей, автоматизацией процессов назначений и отзыва ролей субъектов доступа при наступлении в информационной системе определённых событий, что позволяет совершенствовать модели и расширять области их применения. Однако, в работах недостаточное внимание уделено вопросам аудита, реализованных в системе прав доступа.

Для реализации политик управления доступом наиболее часто используется дискреционная модель разграничения прав доступа в системе, которая должна в результате авторизации пользователя (субъекта доступа) на основании его списка прав ограничивать возможности по доступу и работе с объектами. Однако, в некоторых случаях просто разграничения доступа недостаточно, поскольку возможны ситуации, связанные с несанкционированным повышением привилегий пользователя или ошибками, допущенными в процессе назначения прав доступа. Для предотвращения подобных ситуаций и минимизации их негативных последствий, необходимо периодически проводить аудит событий и действий пользователей связных с доступом к ресурсам, файлам и каталогам в ИИ. Это позволит выявить потенциальные нарушения, инциденты информационной безопасности (ИБ), а также скорректировать политику управления доступом. Концепция подобного подхода к аудиту представлена на Рисунке 1.

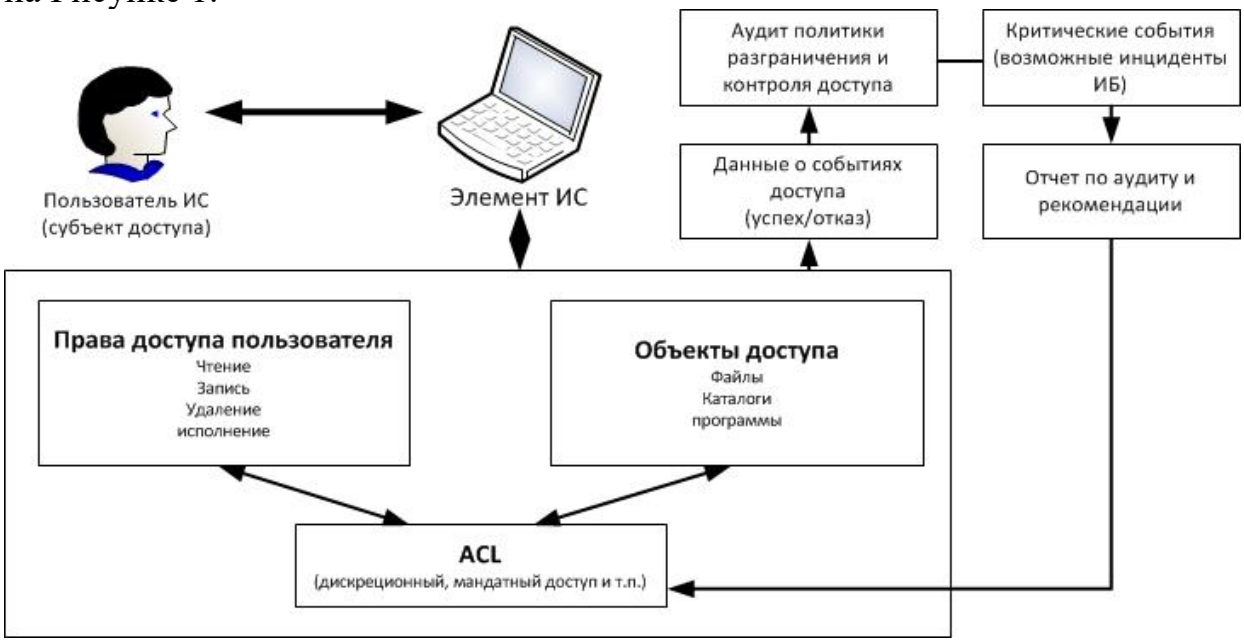

Рисунок 1 - Концепция проведения аудита политики разграничения доступа

Аудит политики разграничения доступа в ИИ проводится в несколько этапов, описание которых представлено в Таблице 1.

Таблица 1 – Этапы проведения аудита политика разграничения доступа

Номер этапа	Название этапа	Работы этапа
Этап 1	Инициирование процедуры аудита	1) Определение элементов ИИ, на которых будет осуществляться аудит. 2) Определение требований к качеству (безопасности) политики разграничения доступа в ИИ. 3) Определение списка субъектов и объектов доступа в ИИ, подлежащих аудиту. 4) Определение ценности и важности объектов доступа в ИИ. 5) Определение источников данных аудита, настройка параметров аудита и действий субъектов над которыми требуется вести аудит.
Этап 2	Сбор информации аудита	1) Для каждого пользователя - субъекта доступа получение данных о правах доступа к каждому объекту доступа на основе информации ACL списков. 2) Получения данных о событиях связанных с разграничением и применением прав доступа субъектов доступа над объектами доступа.
Этап 3	Анализ данных аудита	1) Анализ записей событий и выявление событий, связанных с успешным и неуспешным действием субъектов доступа над объектами. 2) Выделение событий и ситуаций, связанных с неуспешным действием субъектов доступа над объектами, определение источника событий, типа событий (тип действия субъекта), даты и времени наступления событий, анализ частоты появления подобного

		события на установленный период времени. 3) Анализ причин и последствий выявленных неуспешных событий доступа, оценка их опасности. 4) Выявление критичных событий, которые могут быть частью сценария развития инцидента ИБ в ИИ.
Этап 4	Выработка рекомендаций по предотвращению инцидентов ИБ, связанных с выявленными неуспешными событиями доступа и модификации ACL списков.	
Этап 5	Подготовка аудиторского отчета	Формирование документального отчета о результатах, с указанием перечня рекомендаций по достижению требований безопасности и устранению замечаний.

Для описания аудита подсистемы контроля доступа предлагается использовать математическую модель, построенную на применении элементов теории множеств. При разработке модели в качестве базовой модели разграничения доступа, предлагается использовать одну из классических моделей компьютерной безопасности - дискреционную модель Харрисона – Руззо – Ульмана (HRU) [10]. В данной модели для разграничения доступа субъектов доступа к объектам доступа используется матрица, значения элементов которой представляют собой множество базовых прав доступа. К таким правам субъектов доступа к объектам доступа относят: право на чтение, право на запись и изменение, право на исполнение, право на удаление. При разработке математического описания модели аудита подсистемы разграничения доступа, базовые права модели HRU предлагается расширить за счет добавления множества прав, описанных в списках контроля доступа ACL. В результате модель аудита

подсистемы разграничения доступа в ИИ можно представить в виде функции, см. формулу 1.

$$Audit=F(S, O, R, Q, REC), \quad (1)$$

где

S={S1,...Sn}- линейно упорядоченное множество субъектов доступа в ИИ;
O={O1,…Om} - линейно упорядоченное множество объектов доступа в ИИ;
R - Множество прав доступа субъектов доступа по отношению к объектам доступа, сформированные с помощью прав доступа списка ACL;
Q={Q1,..Qz} – множество состояний ИИ.
REC – множество рекомендаций по повышению эффективности политики разграничения доступа к субъектам и объектам доступа в ИИ.

Расширенное множество прав доступа *R* на основе списка ACL для ОС Windows включает в себя следующие элементы:

- до запись данных (data_rec);
- смена разрешений (perm_ch);
- создание папки (dir_cr);
- создание файлов (file_cr);
- удаление (del);
- удаление поддиректорий и файлов (file_dir_del);
- полный доступ (full_acc);
- выполнение файлов (file_ex);
- содержание папки (dir_cont);
- изменение (ch);
- чтение (r);
- чтение и выполнение (r_ex);
- чтение атрибутов (att_r);
- чтение данных (data_r);
- чтение дополнительных атрибутов (ext_att_r);
- чтение разрешений (perm_r);
- смена владельца (own_ch);
- траверс папок (dir_t);
- запись (w);
- запись атрибутов (att_w);
- запись данных (data_w);
- запись дополнительных атрибутов (ext_att_w).

и формализовано записывается как *R={data_rec, perm_ch, dir_cr , file_ch, del, file_dir_del, full_acc, file_ex, dir_cont, ch, r, r_ex, att_r, data_r, ext_att_r, perm_r, own_ch, dir_t, w, att_w, data_w, ext_att_w }.*

Разграничительная политика доступа субъектов к объектам описывается в матрице доступа M, где строки матрицы – это множество субъектов доступа S, столбцы матрицы – множество объектов доступа O, а

значения ячейки матрицы $M = (m_{S,O})$ - набор прав доступа субъектов к объектам доступа, формула 2.

$$M = (m_{S,O})_{\substack{O=\overline{O1,Om} \\ S=\overline{S1,Sn}}} \in R \qquad (2)$$

Множество состояний системы Q в любой момент времени t описывается формулой 3.

$$Q=(S, O, M) \qquad (3)$$

В процессе аудита, для каждого субъекта $S_i \in S$ проверяется, соответствуют ли права, назначенные в ACL выбранного объекта доступа (O_{ACLj}), правам, указанным в профиле данного пользователя. Профиль прав доступа пользователя P_{S_i,O_j} к различным объектам доступа, составляется на базе политики безопасности в области разграничения доступа в ИИ и хранится в виде шаблона в специальной базе данных. Все множество сформированных профилей пользователей, образует "эталонную" матрицу разграничения доступа в системе $P_{S,O}$, которая соответствует безопасному состоянию системы $Q_{SEC}=(S,O,P)$. Таким образом, при аудите подсистемы разграничения доступа происходит последовательный анализ и сопоставление множества значений прав доступа из ячеек матрицы доступа для каждого субъекта $S_i \in S$ и объекта доступа $O_j \in O$. Математически права доступа для каждого субъекта S_i указанные в ACL выбранного объекта O_j (значение конкретной ячейки матрицы доступа M) представляют собой вектор значений, сформированный из элементов множества R. Поэтому при сравнении существующих прав доступа из ACL с правами доступа из профиля используется подход, основанный на вычислении расстояния Хемминга, см. формулу 4.

$$H(Q_T, Q_{SEC}) \qquad (4)$$

Если при сопоставлении прав доступа все в порядке и отклонений в значениях векторов нет, то текущее состояние системы Q_T считается «условно безопасным» Q_{SEC}.

$$H(Q_T, Q_{SEC}) = \begin{cases} 0, \text{отклонений не обнаружено, соответвует ПБ} \\ > 0, \text{есть ошибки, состояние не соответсвует ПБ} \end{cases}$$

По результатам проведенного аудита формируется отчет и рекомендации.

Результаты и обсуждение

Для удобства применения разработанной формализованной модели аудита подсистемы разграничения доступа было разработано программное средство, позволяющее автоматизировать сбор данных и основные этапы

проведения аудита на основе анализа ACL объекта доступа и прав субъекта доступа.

На данный момент исследования программным средством будет анализироваться, и подвергаться аудиту только политика разграничения доступа в ОС семейства Windows, в дальнейшем планируется расширение функциональных возможностей.

Архитектура программного средства представлена на Рисунке 2.

Рисунок 2 – Архитектура программного средства аудита политик разграничения и управления доступа

Графический пользовательский интерфейс предназначен для взаимодействия с пользователем, ввода конфигурационных данных и вывода результата. Работа пользователя с ним будет строиться на принципах, принятых в ОС Windows. Все функциональные возможности программного средства реализованы областью команд и тремя функциональными вкладками (см. Рисунок 3):

1) Вкладка «Добавление».
2) Вкладка «БД».
3) Проверка.

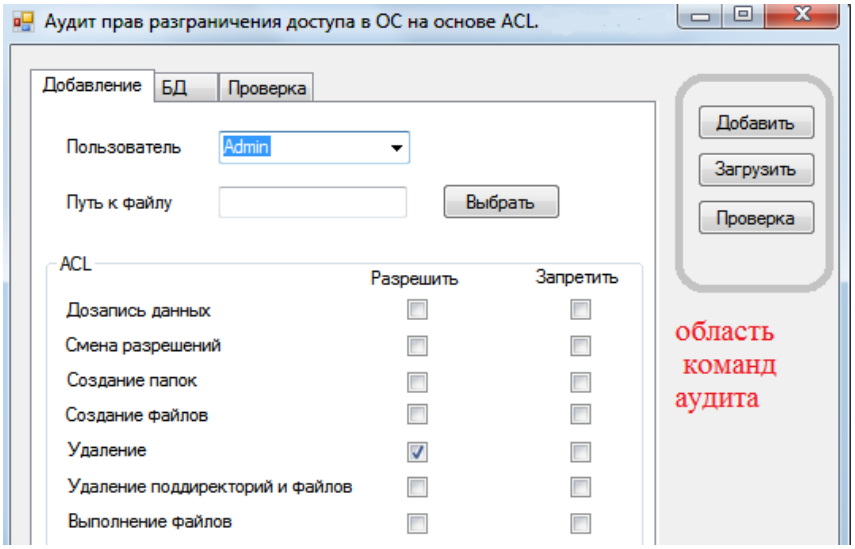

Рисунок 3 - Экранная копия графического пользовательского интерфейса

Модуль сбора данных о субъектах доступа и объектах доступа предназначен для выбора субъектов и объектов политика и права доступа к которым подлежат аудиту. Позволяет сформировать «эталонный» профиль разрешенных и запрещенных прав доступа субъекта (пользователя ОС) к определённому объекту (файлу, каталогу) и сохранить данный профиль в текстовой базе данных.

Модуль анализа ACL выбранного объекта доступа предназначен для получения данных из ACL файла выбранного объекта доступа и формирования списка существующих прав доступа для каждого субъекта ОС.

Модуль аудита предназначен для анализа полученных прав доступа субъектов к объектам доступа. Осуществляет сопоставление значений текущих прав доступа выбранного субъекта из ACL с «эталонными» правами доступа этого же субъекта из профиля в БД. Выводит результат сравнения и список несоответствий политики разграничения доступа.

Заключение

В целях обеспечения требуемого уровня информационной безопасности данных и ИИ требуется не только обеспечивать защиту информационных ресурсов, но и контролировать эффективность и работоспособность подсистем информационной безопасности.

В результате исследований были решены частные задачи:

1) разработана и поэтапно описана схема концепции проведения аудита политики разграничения доступа;
2) представлено математического описание процедуры аудита политики управления и разграничения доступа пользователей на основе дискреционной модели;

4. разработан прототип программного инструмента с графическим пользовательским интерфейсом, для проведения аудита политики управления доступом в ОС Windows.

Предлагаемый подход к аудиту подсистемы управления доступом в информационной системе позволит осуществлять периодический контроль за состоянием настроек и прав доступа субъектов к объектам информационной системы, выявлять несоответствия существующих прав управления доступом и ACL листов политики информационной безопасности, а, следовательно, своевременно применять меры по их устранению, что приведет к снижению уровня потенциального риска. В дальнейшем планируется доработка функциональных возможностей и совершенствование инструментального средства аудита.

ЛИТЕРАТУРА

1. Аналитический отчет Positive Technologies «Актуальные киберугрозы — 2018. Тренды и прогнозы». - https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/ (дата обращения 15.03.2019).
2. Витенбург Е.А., Никишова А.В. Структура информационной системы предприятия как основа формирования системы защиты информации// Информационные технологии в науке, образовании и производстве (ИТНОП-2018) VII Международная научно-техническая конференция. Сборник трудов конференции. 2018. С. 162-167.
3. Булгаков О.М., Удалов В.П., Четкин О.В. Математическая модель воздействия нарушителя на компоненты интегрированной системы безопасности// Вестник Воронежского института МВД России. 2015. №2. С. 165 – 175. - http://cyberleninka.ru/article/n/matematicheskaya-model-vozdeystviya-narushitelya-na-komponenty-integrirovannoy-sistemy-bezopasnosti (дата обращения 28.02.2019).
4. Оладько В.С. Риски систем управления и контроля доступа// Молодой ученый. 2016. №28 (132). С. 133 – 136/
5. Токарев В.Л., Сычугов А.А. Метод аудита защищенности автоматизированных систем// Моделирование, оптимизация и информационные технологии. Научный журнал, 2019. Том 7. №1. - http://moit.vivt.ru (дата обращения 28.02.2019).
6. Семенова Н.А. Семантическая модель управления доступом//Прикладная дискретная математика.2012.№2(16). С. 50-64.
7. Колегов Д.Н., Ткаченко Н.О. Легковесная реализация механизма атрибутного управления доступом для СУБД на уровне защитного экрана//Прикладная дискетная математика. Приложение. 2016. С.93 – 95.

8. Миронова В. Г., Шелупанов А.А. Анализ режимов разграничения и распространения прав доступов на основе дискреционной модели разграничения прав доступов Take-Grant// Известия Южного федерального университета. Технические науки. 2013. №12 (149).С. 111 – 117.
9. Куракин А.С., Костырева А.А. Модель разграничения прав доступа для информационной системы специального назначения//Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 2. С. 82-89. doi: 10.24411/2409-5419-2018-10262
10. Чиркова М.Л., Шубин Е.В. Применение модели HRU для обеспечения безопасности информационных систем// Всероссийская ежегодная научно-практическая конференция: сборник материалов, г. Киров 15-26 апреля 2013. С. 513-515.

V. S Oladko

FORMALIZATION OF THE ACCESS CONTROL AUDIT PROCEDURE IN THE INFORMATION SYSTEM

Financial University under the Government of the Russian Federation
Moscow, Russia

The article discusses current problems and tools for ensuring information security in information systems. The author analyzes the current trends in information security breaches in 2018-2019, concludes about the relevance of countering threats related to unauthorized access. The basic tools for protecting an information system from unauthorized access are many rights and rules for access control between objects and subjects. Therefore, to ensure the necessary level of security, the adequacy and consistency of the distribution of access rights is important. The methodology and conceptual scheme for conducting an audit of the access control subsystem based on ACL lists, consisting of procedures for initiating audits, collecting and analyzing audit data has been developed. The mathematically model of audit procedure is automation in the form of an audit software tool for the access control subsystem using the Windows operating system as an example. The main advantage of the proposed audit procedure is that it does not require complex testing procedures, calculation of probabilities, involvement and selection of experts. The main purpose of the program is to assess the compliance of the existing settings of the access control policy in the system with the security policy of the system under investigation.

Keywords: access rights, information protection, operating system, access control model, mathematical model, cybersecurity.

REFERENCES

1. Analytical report of Positive Technologies “Actual cyber threats - 2018. Trends and forecasts”. - https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/ (appeal date 03/15/2019).
2. Vitenburg E.A., Nikishova A.V. The structure of the information system of the enterprise as a basis for the formation of the information security system // Information technologies in science, education and production (ITNOP-2018) VII International Scientific and Technical Conference. Collection of conference proceedings. 2018. pp. 162-167.
3. Bulgakov OM, Udalov VP, Chetkin OV Mathematical model of the impact of the offender on the components of the integrated security system // Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia, 2015.№2. Pp. 165 - 175. - http://cyberleninka.ru/article/n/matematicheskaya-model-vozdeystviya-narushitelya-na-komponenty-integrirovannoy-sistemy-bezopasnosti (appeal date 02/28/2019).
4. Oladko V.S. Risks of control and access control systems // Young Scientist. 2016. №28 (132). P. 133 – 136. Tokarev V.L., Sychugov A.A. Method of Auditing the protection of automated systems // Modeling, optimization and information technology. Scientific journal, 2019. Volume 7. №1. - http://moit.vivt.ru (circulation date 02/02/2019).
5. Tokarev V.L., Sychugov A.A. Method of audit protection of automated system// Modeling, Optimization and Information Technology” (“MOIT”). 2019. T.7. №.1.
6. Semenova N.A. Semantic model of access control // Applied Discrete Mathematics. 2012.№2 (16). S. 50-64. (In Russia)
7. Kolegov D.N., Tkachenko N.O. Lightweight implementation of attribute access control mechanism for DBMS at the level of a protective screen // Applied diskette mathematics. Application. 2016. S.93 - 95. (In Russia)
8. Mironova V.G., Shelupanov A.A. Analysis of differentiation and distribution of access rights based on the discretionary model of differentiation of access rights Take-Grant // Bulletin of the Southern Federal University. Technical science. 2013. No. 12 (149) .C. 111 - 117. (In Russia)
9. Kurakin A.S., Kostyreva A.A. Model of limitation of rights of access for special purpose information system. H&ES Research. 2019. Vol. 11. No. 2. Pp. 82–89. doi: 10.24411/2409-5419-2018-10262 (In Russia)
10. Chirkova M.L., Shubin E.V. The use of the HRU model to ensure the security of information systems // All-Russian annual scientific-practical conference: collection of materials, Kirov April 15-26, 2013. P. 513-515.