*Чадов А. Ю., МФТИ*

**Децентрализованная система разграничения доступа**

1. **Введение**

 Одной из основных задач защиты информации является разграничение доступа. На данный момент уже существует большое количество различных систем разграничения доступа к информации, среди основных решений на рынке СЗИ от НСД можно выделить следующие наиболее распространенные продукты:

 Secret Net («Код Безопасности»): степень охвата рынка – 52%

 «Аккорд» (ОКБ САПР): степень охвата рынка – 25,8%

 Dallas Lock («Конфидент»): 5,8 % [1]

Во всех этих решениях система, принимающая решения о запрете или разрешении доступа, располагается на самом подконтрольном объекте (ПКО), таким образом машина, отвечающая за обработку данных, отвечает и за безопасность [2, 3, 4, 5, 6, 7].

Проанализируем, что будет, если построить систему, в которой эти функции выполняют разные машины.

В данной статье описывается концепция новой системы разграничения доступа, в которой элемент, отвечающий за приятие решений о разрешении доступа вынесен на другую машину.

1. **Проектирование новой системы**

При создании концепции новой системы, сначала определим модель контроля доступа, которая будет использоваться в новой системе. Наиболее популярными и распространёнными в данный момент являются подход к разграничению доступа на основе ролей (Role-Based Access Control, RBAC) [8] и подход к разграничению доступа на основе атрибутов (Attribute-Based Access Control, ABAC) [9]. Но роль в понимании стандарта RBAC может быть назначена субъекту в рамках ABAC в качестве одного из атрибутов, что делает RBAC в некотором смысле частным случаем и лишает его перед ABAC всех преимуществ [10]. Поэтому новая система должна базироваться на атрибутной модели контроля доступа.

Далее нужно определить архитектуру новой системы. В спецификации NIST стандарта ABAC приведены два варианта архитектуры системы для двух стандартов XACML и NGAC:



*Рис. 1. Функциональная архитектура NGAC [11]*



*Рис. 2. Функциональная архитектура XACML [11]*

В обоих вариантах предложена модульная система. Модульные системы обладают рядом достоинств: возможность резервного дублирования отдельных критичных модулей, лёгкая заменимость модулей при необходимости, удобное управление и настройка.

В соответствии со стандартом, нашу новую систему тоже сделаем модульной. В новой системе элемент, отвечающий за принятие решений будет вынесен на отдельную рабочую станцию. При этом на ПКО должен остаться агент, перехватывающий запросы субъектов к объектам и отправляющий их к удалённому элементу, принимающему решения о доступе. Поскольку модуль принятия решений вынесен отдельно, имеет смысл сделать его одним для всех ПКО, контролируемых данной системой разграничения доступа в рамках одной информационной системы, чтобы избежать ненужного дублирования.

Модульная система разграничения доступа будет более универсальной: если, например, ОС на рабочих станциях нужно будет сменить на несовместимую с модулем перехвата данных, достаточно будет сменить только этот модуль на совместимый с нужной ОС.

Мы выделили два элемента, которые должны быть в новой системе разграничения доступа. В стандарте в обеих архитектурах помимо уже обозначенных модулей есть отдельный модуль хранения политик доступа и модуль управления политиками. Включим их новую систему. Итак, среди модулей в новой системе должны быть: модуль приятия решений о доступе, модуль хранения политик доступа, модуль-перехватчик запросов доступа субъектов к объектам, модуль управления политиками. Также нужна транспортная система для передачи сообщений между модулями и хранения их в очередях в случае необходимости — она так же должна являться модулем. При дальнейшем развитии можно будет при необходимости добавлять новые модули, например, систему журналирования тоже можно вынести в отдельный модуль.

1. **Трудности, возникающие при построении модульной системы**

Сама концепция модульной системы привносит особенности, которые необходимо учитывать.

 Первое – если решения теперь принимаются на удалённой машине, то ко времени принятия решения о предоставлении доступа добавится время на передачу сообщений между модулями, как следствие может возрасти время отклика системы. При проектировании нужно учесть особенности передачи данных по сети и минимизировать задержку. Возможно, для этого придётся объединять некоторые модули в рамках одной рабочей станции, либо делать локальный кэш. *Задержка работы системы не должна превышать времени чтения данных с диска.* Современные сетевые технологии позволяют построить такую систему – задержка передачи по сети достаточно мала по сравнению со скоростью чтения данных с диска [12].

 Второе – защита данных, передаваемых между модулями. Поскольку теперь части системы разграничения доступа находятся не в рамках одной рабочей станции, то для некоторых типов сообщений (нужно исследовать для каких именно), *придётся обеспечивать конфиденциальность или целостность данных*. Для этого можно использовать шифрование, подпись либо протоколы защиты канала. Следует учесть, что всё это также повлияет на скорость отклика и должно быть учтено в проектировании. Также нужно *предусмотреть механизм аутентификации элементов при общении друг с другом*.

1. **Требования к системе и пример архитектуры**



*Рис. 3. Пример того, как может выглядеть новая система*

В данном примере, все модули общаются друг с другом через менеджер сообщений. Работа строится следующим образом: сначала администратор через АРМ управления настраивает базу данных политик. Затем, в процессе работы, агенты, перехватывая события обращаются к серверу принятия решений. Он делает запрос в БД политик, и на основе полученных оттуда данных даёт агенту ответ.

В итоговом варианте схемы могут добавиться новые модули, может появиться локальный кэш на ПКО, что приведёт к изменению схемы работы с системой.

Итак, суммируя сказанное выше, мы получили следующий список требований к новой системе разграничения доступа:

1. Система должна состоять отдельных модулей, общающихся друг с другом через определённое API. Серди этих модулей обязательно должны быть модуль приятия решений о доступе, модуль хранения политик доступа, модуль-перехватчик запросов доступа субъектов к объектам, модуль управления политиками, модуль транспортной системы для передачи сообщений.
2. Решения о доступе субъектов к объектам принимает центральный модуль, политики так же хранятся централизовано.
3. Задержка, вносимая работой системы не должна ощущаться пользователем: она должна быть того же порядка, что и время обращения к диску или меньше.
4. Модули должны уметь проводить взаимную аутентификацию.
5. Данные, передаваемые в запросах модулей друг к другу должны быть защищены.

В дальнейшей работе планируется исследовать вопросы, поднятые в главе 3: безопасность и быстродействие системы. Нужно исследовать на какое будет время отклика у такой системы, исследовать какие методы защиты данных нужно применить в этой системе и для каких именно данных. Нужно так же проработать технические моменты реализации агента: к примеру, при генерации события доступа субъекта к объекту, агент должен будет отправить запрос к модулю принятия решений, а для этого агенту нужно будет получить доступ к сетевым ресурсам, что сгенерирует событие доступа. Такие технические особенности нужно учесть, возможно это повлияет на архитектуру решения. С учётом результатов этих исследований можно будет приступить к созданию итогового проекта.

**Список литературы.**

1. *Комаров А.* Рынок систем защиты информации (СЗИ) от несанкционированного доступа (НСД) в России. 2013 [Электронный ресурс]. URL: https://www.anti-malware.ru/node/11728# (дата обращения: 02.04.2018).
2. Документы Компании «Код безопасности»: Средство защиты информации SecretNet 7. Руководство администратора. Принципы построения [Электронный ресурс]. URL: https://www.securitycode.ru/upload/documentation/secret\_net/Secret\_Net\_Admin\_Guide\_Construction\_Principles.pdf (дата обращения: 15.03.2018).
3. Документы Компании «ОКБ САПР»: Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «АККОРД-Win32» (версия 4.0). Описание применения [Электронный ресурс]. URL: http://www.accord.ru/accwin32-prim.html (дата обращения: 15.03.2018).
4. Документы Компании «ОКБ САПР»: Система удаленного централизованного управления СЗИ от НСД АККОРД. Руководство Администратора [Электронный ресурс]. URL: http://www.accord.ru/accwin32-admin.html (дата обращения: 15.03.2018).
5. Документы Компании «ОКБ САПР»: СУЦУ [Электронный ресурс]. URL: http://www.accord.ru/sucu.html (дата обращения: 15.03.2018).
6. Документы Центра защиты информации ООО «Конфидент»: Система защиты информации от несанкционированного доступа «Dallas Lock 8.0-К». Описание применения [Электронный ресурс]. URL: https://www.dallaslock.ru/upload/medialibrary/cp/documents/RU.48957919.501410-01%2031%20-%20Описание%20применения%20DL%208.0-K.pdf (дата обращения: 15.03.2018).
7. Документы Центра защиты информации ООО «Конфидент»: Система защиты информации от несанкционированного доступа «Dallas Lock 8.0-К». Руководство по эксплуатации [Электронный ресурс]. URL: https://www.dallaslock.ru/upload/medialibrary/cp/documents/RU.48957919.501410-02%2092%20-%20Руководство%20по%20эксплуатации.pdf (дата обращения: 20.11.2016).
8. *Ferraiolo D., Kuhn R.* Role-Based Access Controls // Proceedings of the 15th National Computer Security Conference. Gaithersburg: NIST Gaithersburg MD, 1992. Р. 554–563.
9. *Sandhu R., Ferraiolo D., Kuhn R.* The NIST model for role-based access control: towards a unified standard // Proceedings of the 5th ACM Workshop on Role-based Access Control. NY: ACM New York, 2000. P. 47–63.
10. *Coyne E., Weil T. R.* ABAC and RBAC: Scalable, Flexible, and Auditable Access Management // IT Professional. 2013. № 3. P. 14-16.
11. *Ferraiolo D., Chandramouli R., Hu V., Kuhn R.* NIST Special Publication 800-178 A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications P. 21, 34
12. Latency Numbers Every Programmer Should Know [Электронный ресурс] URL: <https://gist.github.com/jboner/2841832> (дата обращения: 01.04.18).