Лабораторная работа №2
«Active Directory. Аутентификация в сетях Windows»

«25» февраля 2021 г.

Москва 2021 г.

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Информация – сведения (сообщения, данные) независимо от формы их представления [1].

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [1].

Конфиденциальность – свойство конкретной информации быть доступной только тому кругу лиц, для которого она предназначена.

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Доступность – возможность за приемлемое время получить требуемую информацию легальному пользователю.

Авторство (**Аутентичность**) – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор.

Неотказуемость от авторства – невозможность автора отказаться от авторства.

Информационная безопасность – это свойство информации сохранять конфиденциальность, целостность, доступность, авторство и неотказуемость от авторства. Угрозой нарушения безопасности считается угроза нарушения одного из свойств безопасности информации.

Active Directory (AD) – реализация Windows службы каталогов общего назначения, которая использует LDAP в качестве основного протокола доступа [].

Каталог – база данных, в которой хранится информация об объектах, таких как пользователи, группы, компьютеры, принтеры, и служба каталогов, которая делает эту информацию доступной для пользователей и приложений [].

Контроллер домена (DC) – служба, работающая на сервере, реализующая Active Directory, или сервер, на котором размещена эта служба. Служба размещает

хранилище данных для объектов и взаимодействует с другими контроллерами домена, чтобы гарантировать правильную репликацию локального изменения объекта на всех контроллерах домена.

Атрибут – идентификатор для однозначного или многозначного элемента данных, который связан с объектом каталога []. Объект состоит из его атрибутов и их значений. Примеры в AD: CN (обычное имя), street (почтовый адрес) и mail (адреса электронной почты) могут быть атрибутами объекта пользователя. Схема атрибута, включая синтаксис его значений, определяется в объекте attributeSchema.

Домен AD – набор пользователей и компьютеров, совместно использующих общее пространство имен и инфраструктуру управления []. По крайней мере, один компьютер, входящий в набор, должен действовать как контроллер домена (DC) и содержать список членов, который идентифицирует всех членов домена, а также необязательно размещать службу Active Directory. Контроллер домена обеспечивает аутентификацию участников, создавая единицу доверия для своих членов. У каждого домена есть идентификатор, который совместно используется его членами.

Лес AD – один или несколько доменов, которые имеют общую схему и транзитивно доверяют друг другу []. В организации может быть несколько лесов. Лес устанавливает границы безопасности и административные границы для всех объектов, находящихся в доменах, принадлежащих лесу (в то время как домен устанавливает административную границу для управления объектами, такими как пользователи, группы и компьютеры). Кроме того, каждый домен имеет индивидуальные политики безопасности и доверительные отношения с другими доменами.

Групповая политика – механизм, который позволяет разработчику указывать управляемые конфигурации для пользователей и компьютеров в среде службы Active Directory [].

GSS-API – стандарт Интернета, описанный в [RFC2743], для предоставления услуг безопасности приложениям []. Он состоит из набора интерфейса прикладного программирования (GSS-API), а также стандартов, описывающих структуру данных безопасности.

SRV – запись ресурса системы доменных имен (DNS), используемая для идентификации компьютеров, на которых размещены определенные службы, как указано в [RFC2782 – спецификация DNS SRV]. Записи ресурсов SRV используются для поиска контроллеров домена (DC) для Active Directory [].

Service principal name (SPN) – имя, которое клиент использует для идентификации службы для взаимной аутентификации. SPN состоит из двух или трех частей, каждая из которых разделена косой чертой ('/'). Первая часть – это класс службы, вторая часть – имя хоста, а третья часть (если есть) – имя службы. Например, «ldap/dc-01.fabrikam.com/fabrikam.com» – это имя участника-службы, состоящее из трех частей, где «ldap» – это имя класса службы, «dc-01.fabrikam.com» – имя хоста, а «fabrikam.com» – это название службы [].

User principal name (UPN) – имя учетной записи пользователя (иногда называемое именем пользователя для входа в систему) и имя домена, которое идентифицирует домен, в котором находится учетная запись пользователя. Это стандартное использование для входа в домен Windows. Формат: something@example.com (в виде адреса электронной почты). В Active Directory – атрибут userPrincipalName объекта учетной записи, как описано в [MS-ADTS – главная спецификация Active Directory].

Digest-аутентификация – протокол, который использует механизм запроса-ответа для проверки подлинности, в котором клиенты могут проверять свою личность, не отправляя на сервер открытый пароль [].

NT LAN Manager (NTLM) – протокол аутентификации, основанный на последовательности запрос-ответ для аутентификации [].

Kerberos – система аутентификации, которая позволяет двум сторонам обмениваться частной информацией через открытую сеть, назначая уникальный ключ (называемый билетом) каждому пользователю, который входит в сеть, а затем встраивает эти билеты в сообщения, отправленные пользователями [].

Key Distribution Center (KDC) – служба Kerberos, которая реализует службы проверки подлинности и выдачи билетов, указанные в протоколе Kerberos. Служба

работает на компьютерах, выбранных администратором области или домена; он присутствует не на всех машинах в сети. У него должен быть доступ к базе данных учетных записей той области, которую он обслуживает. KDC интегрированы в роль контроллера домена. Это сетевая служба, которая предоставляет клиентам билеты для использования при аутентификации служб [].

Ticket-Granting Ticket (TGT) – специальный тип билета, который можно использовать для получения других билетов []. TGT получается после начальной аутентификации в обмене службой аутентификации (AS); после этого пользователям не нужно представлять свои учетные данные, но они могут использовать TGT для получения последующих билетов.

Ticket-Granting Service (TGS) – 1) служба, которая выдает билеты для доступа к другим службам в своем собственном домене или для доступа к службе выдачи билетов в другом домене (официальное определение Microsoft) [];

2) специальный тип билета, который можно использовать для обращения к конкретной службе.

ОС – операционная система.

ПО – программное обеспечение.

ВМ – виртуальная машина.

1 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.1 Active Directory

1.1.1 Общие положения

Для управления компьютерной сетью с рабочими станциями, серверами разветвленной топологией возникает необходимость в централизованном хранении информации обо всех объектах сети. Традиционный способ обращения с колоссальным объемом информации о сетевых ресурсах — хранение ее в отдельных каталогах, которые обычно управляются приложением или компонентом операционной системы, использующим эту информацию.

Службы каталогов в сетевых ОС применяются достаточно давно. Так, в типичной сети на основе Windows NT 4.0 (ОС предшествующая Windows 2000) вы могли бы обнаружить несколько каталогов с информацией, разбросанной по серверам этой сети. Списки пользователей и управления доступом хранились в каталоге, который назывался базой данных Security Accounts Manager (SAM). Почтовые ящики Exchange Server и их сопоставления с пользователями размещались в каталоге Exchange. Прочие службы и приложения поддерживали свои каталоги. Хотя взаимодействие между этими каталогами в какой-то мере было возможным, но по большей части они были изолированными.

Чаще всего каталоги разрабатывались под конкретные приложения, на тот момент так было проще. Однако с ростом сетей, администраторы и пользователи были вынуждены выполнять все больше и больше работы, отчаянно нуждались в том, чтобы все эти раздельные базы данных могли взаимодействовать между собой, и чтобы, ими можно было управлять как единым целым.

Такой универсальный каталог был разработан компанией Microsoft для операционной системы Windows 2000, а в Windows 2003 был применен более усовершенствованный вариант Active Directory.

В сложной сети служба каталогов должна обеспечивать эффективный способ управления, поиска и доступа ко всем ресурсам в этой сети, например, к компьютерам, принтерам, общим папкам и т. д. Хорошая реализация службы каталогов дает следующие основные преимущества.

1. Централизация. Смысл централизации — уменьшение количества каталогов в сети. Включение информации обо всех сетевых ресурсах в централизованный каталог создает единственную точку управления, что упрощает администрирование ресурсов и позволяет эффективнее делегировать административные задачи. Кроме того, в сети появляется единая точка входа для пользователей (или их компьютеров/приложений), когда возникает необходимость в поиске ресурсов.

2. Масштабируемость. Служба каталогов должна допускать рост сети, не создавая при этом слишком больших издержек. То есть она должна поддерживать какой-либо способ разбиения базы данных каталога на разделы, чтобы не утратить контроль над базой данных из-за ее чрезмерного разрастания и при этом сохранить преимущества централизации.

3. Стандартизация. Служба каталогов должна предоставлять доступ к своей информации по открытым стандартам. Это гарантирует, что другие приложения смогут использовать ресурсы в Active Directory (и публиковать их в ней), а не поддерживать собственные каталоги.

4. Расширяемость. Служба каталогов должна тем или иным способом позволять администраторам и приложениям расширять в соответствии с потребностями организации набор информации, хранимой в каталоге.

5. Разделение физической сети. Благодаря службе каталогов топология физической сети должна быть траспарентной пользователям и администраторам. Ресурсы можно находить (и обращаться к ним), не зная, как и где они подключены к сети.

6. Безопасность. Служба каталогов была бы крайне полезной злоумышленнику, так как она хранит подробную информацию о данной организации. Поэтому служба каталогов должна поддерживать защищенные средства хранения, управления, выборки и публикации информации о сетевых ресурсах.

1.1.2 Логическая и физическая структура AD

Active Directory содержит две структуры- логическую и физическую. Логическая структура состоит из доменов, подразделений, лесов и деревьев, тогда как физическая структура содержит специальные серверы, называемые контроллерами домена, и сайты.

1.1.2.1 Логическая структура AD

1.1.2.1.1 Домен AD

Ядро Active Directory составляют домены. Домены представляют собой логические группы компьютеров, определенные сетевым администратором. Компьютеры домена используют единые политики безопасности и могут обмениваться данными с компьютерами в других доменах. Домен, главным образом, представляет собой метод организации административной безопасности. Компьютер, на котором работает сервер каталога, называется контроллером домена; иными словами, контроллер домена — это компьютер, на котором размещена вся база данных Active Directory. Все запросы к активному каталогу и вообще все запросы, касающиеся доступа к информации, хранящейся в домене, обрабатывает именно контроллер домена.

Роль управления доменом — настолько важная в сети функция, что от нее напрямую зависит работа сети. Поэтому и доступ к контроллерам домена (DC, Domain Controller) разрешается с большей осторожностью, чем к остальным, а сами эти компьютеры имеют большую степень безопасности (как с точки зрения сетевого доступа, так и чисто физически) и оснащаются самым надежным оборудованием. В крупных сетях они никогда не выполняют дополнительных серверных функций (не

бывают серверами печати, приложений, файловыми серверами и т.п.). Реализация доменной модели сети начинается с установки контроллера домена.

Для повышения надежности доменной сети, могут быть установлены резервные контроллеры домена. На каждом контроллере домена хранится своя копия базы данных Active Directory. Актуальность копий баз данных Active Directory поддерживается за счет режима репликации. Таким образом, каждый контроллер домена хранит одни и те же данные, включая учетные записи пользователей. Теперь, если один из контроллеров домена выйдет из строя, клиенты автоматически переключатся на другой, и это нисколько не помешает их работе.

1.1.2.1.2 Дерево AD

Если в вашей организации несколько доменов, у вас есть две возможности их логической организации. Первая из них называется деревом доменов. Дерево (tree) - иерархическая структура, включающая в себя несколько доменов с единым пространством имен. Имена объектов должны быть уникальными в пределах всего дерева. Достигается эта уникальность тем, что полное имя подчиненного домена (europe.microsoft.com) складывается из его собственного имени (europe) и имени вышестоящего домена (microsoft.com) (Рисунок 1).

Первый домен, созданный в дереве, является корневым. Следующий домен считается дочерним по отношению к корневому. Имя домена высшего уровня (корневого домена) входит в имена всех поддоменов. На количество доменов, образующих дерево, ограничений нет. Даже если в организации лишь один домен, у вас все равно имеется дерево.

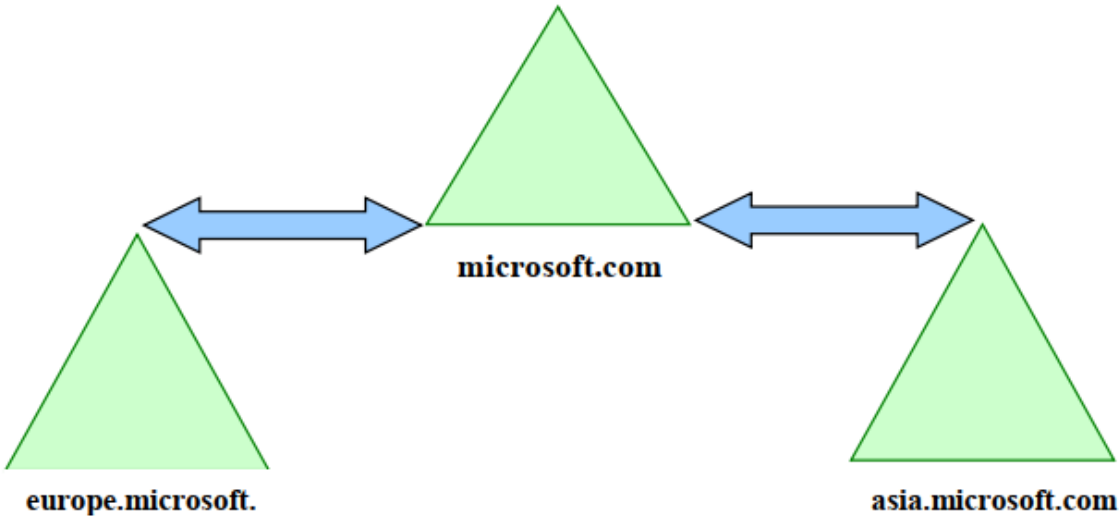

Рисунок 1 – Дерево Microsoft.com

1.1.2.1.3 Лес AD

Другая модель логической организации доменов — лес. Лес — это группа из одного или более деревьев доменов, которые не образуют непрерывного пространства имен, но могут совместно использовать общую схему и глобальный каталог. В сети всегда есть минимум один лес, и он создается, когда в сети устанавливается первый компьютер с поддержкой Active Director (контроллер домена). Первый домен в лесу, называемый корневым доменом леса (forest root domain), играет особую роль, так как на нем хранится схема, и он управляет именованием доменов для целого леса. Его нельзя удалить из леса, не удалив сам лес. Кроме того, в иерархии доменов леса нельзя создать домен, который находился бы над корневым.

На рис. 2 показан пример леса с двумя деревьями. У каждого дерева в лесу свое пространство имен. В данном случае microson.com — это одно дерево, а contoso.com — другое. Оба дерева находятся в лесу с именем microsoft.com.

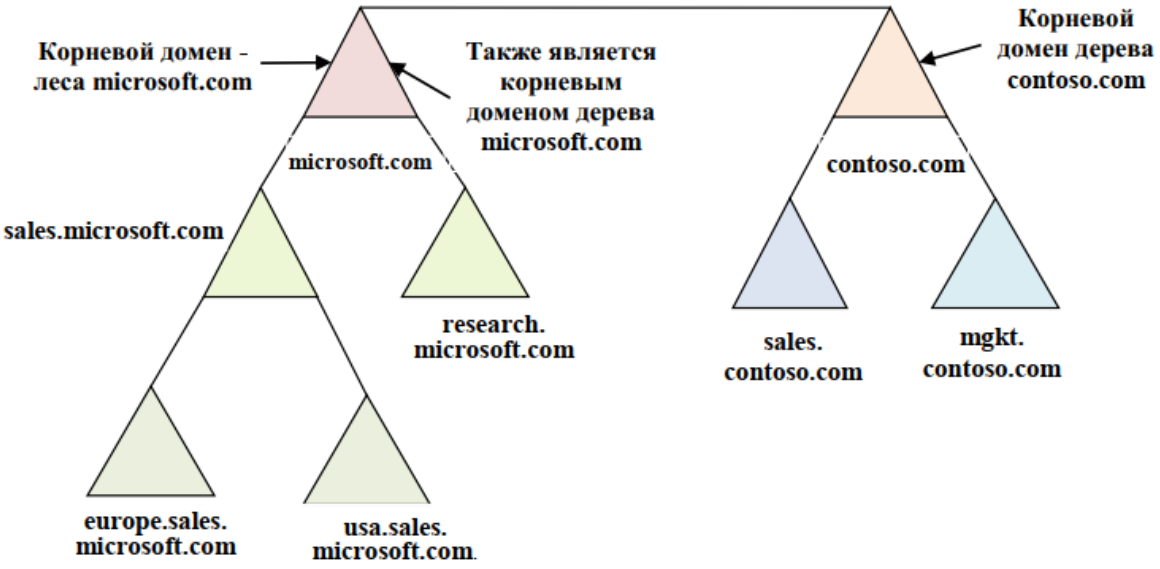

Рисунок 2 – Лес с двумя деревьями

1.1.2.1.4 Организационные единицы

Организационные единицы (organizational units, OU) позволяют разделять домен на зоны административного управления, т. е. создавать единицы административного управления внутри домена. В основном это дает возможность делегировать административные задачи в домене. До появления Active Directory домен был наименьшим контейнером, которому вы могли бы назначить административные разрешения. То есть, передать группе администраторов контроль над конкретным ресурсом было затруднительно или вообще невозможно, не предоставив им широких полномочий во всем домене.

OU служит контейнером, в который можно поместить какие-либо ресурсы домена. После этого вы назначаете административные разрешения самой OU. Обычно структура OU соответствует функциональной или бизнес-структуре организации. Например, в сравнительно небольшой организации с единственным доменом можно было бы создать отдельные OU для отделов этой организации.

OU поддерживают вложение (создание OU внутри другой OU), что обеспечивает более широкие возможности в управлении ресурсами. Однако чрезмерно сложная структура OU внутри домена имеет свои недостатки. Ведь чем проще структура,

тем легче реализация этой структуры и управление ею. Необходимо также учитывать, что, начиная примерно с 12-го уровня вложения OU, возникают серьезные проблемы с производительностью.

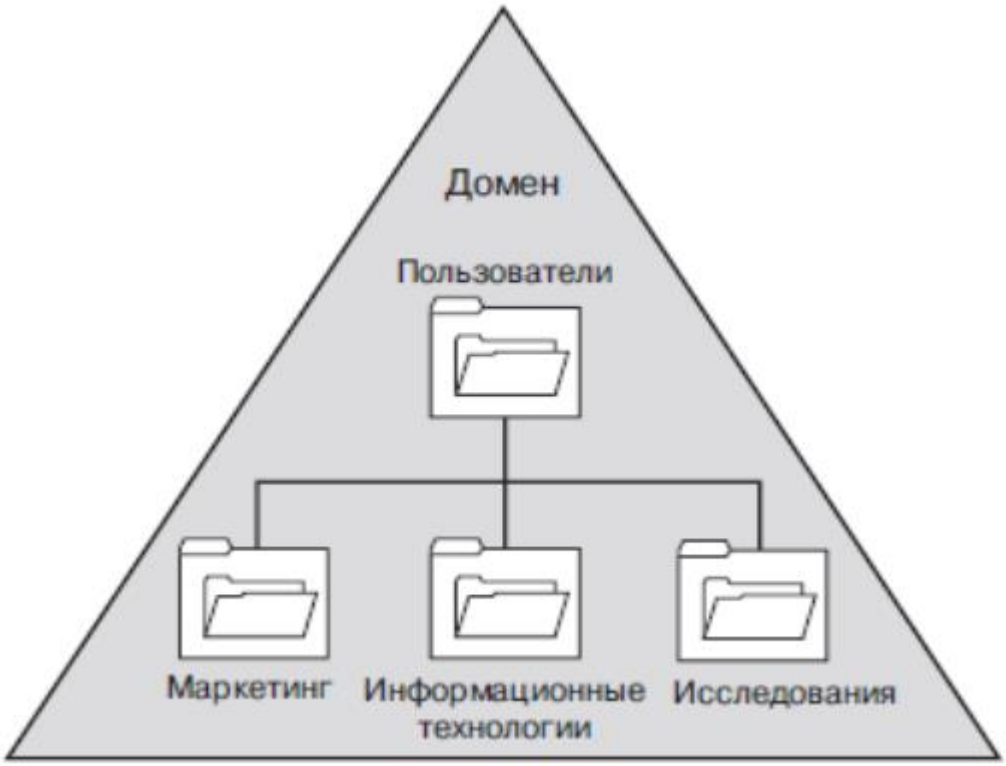

Рисунок 3 – Организационные единицы

1.1.2.2 Физическая структура AD

Контроллер домена — это сервер под управлением Windows Server, на котором установлена и работает служба Active Directory. В домене можно создать любое число контроллеров. На каждом контроллере домена хранится полная копия раздела каталога данного домена. Контроллеры домена локально разрешают запросы на информацию об объектах в своем домене и пересылают в другие домены запросы на информацию, отсутствующую в данном домене. Контроллеры домена также отслеживают изменения в информации каталога и отвечают за репликацию этих изменений на другие контроллеры. А раз каждый контроллер домена хранит полную копию раздела каталога для своего домена, это означает, что контроллеры следуют модели репликации с несколькими хозяевами (multimaster model). То есть каждый контроллер просто

хранит мастер-копию раздела, и с его помощью можно модифицировать эту информацию.

Однако есть роли, которые могут быть присвоены контроллерам домена и при которых выбранный контроллер становится единственным, кому дозволено выполнять упомянутую выше задачу. К таковым относятся роли хозяина операций (operations master roles). Роли, действующие в границах леса. Существует две роли хозяина операций, которые могут быть назначены единственному контроллеру домена в лесу.

- Хозяин схемы (Schema Master). Первый контроллер домена в лесу принимает роль хозяина схемы и отвечает за поддержку и распространение схемы на остальную часть леса. Он поддерживает список всех возможных классов объектов и атрибутов, определяющих объекты, которые находятся в Active Directory. Если схему нужно обновлять или изменять, наличие Schema Master обязательно.
- Хозяин именования доменов (Domain Naming Master). Протоколирует добавление и удаление доменов в лесу и жизненно необходим для поддержания целостности доменов. Domain Naming Master запрашивается при добавлении к лесу новых доменов. Если Domain Naming Master недоступен, добавление новых доменов невозможно; однако при необходимости эта роль может быть передана другому контроллеру.

Сервер глобального каталога – одна из функций сервера, которую можно назначить контроллеру домена. Сервер глобального каталога поддерживает подмножество атрибутов объектов Active Directory, к которым чаше всего обращаются пользователи или клиентские компьютеры, например, регистрационное имя пользователя. Серверы глобального каталога выполняют две важные функции. Они дают возможность пользователям входить в сеть и находить объекты в любой части леса.

Глобальный каталог содержит подмножество информации из каждого доменного раздела и реплицируется между серверами глобального каталога в домене. Когда пользователь пытается войти в сеть или обратиться к какому-то сетевому ресурсу из

любой точки леса, соответствующий запрос разрешается с участием глобального каталога. Без глобального каталога этот запрос мог бы долго передаваться от одного контроллера домена к другому. Если в вашей сети один домен, необходимости в этой функции глобального каталога нет, так как информация обо всех пользователях и объектах сети находится на любом контроллере домена. Но при наличии нескольких доменов функция глобального каталога становится важной.

1.1.3 Аутентификация в AD

Существует несколько протоколов, описывающих процесс аутентификации субъектов в локальной сети. Например, в рамках операционных систем семейства Windows компании Microsoft использовались протоколы LAN Manager (LANMAN), NT LAN Manager (NTLM), NT LAN Manager версии 2 (NTLM v2) и Kerberos.

1.1.3.1 NTLM

LANMAN протокол был одним из первых протоколов аутентификации в Windows. Работает он по принципу «negotiate-challenge» в двухстороннем формате без третьей доверенной стороны. В настоящее время считается небезопасным из-за слабого хеширования (Рисунок 4).

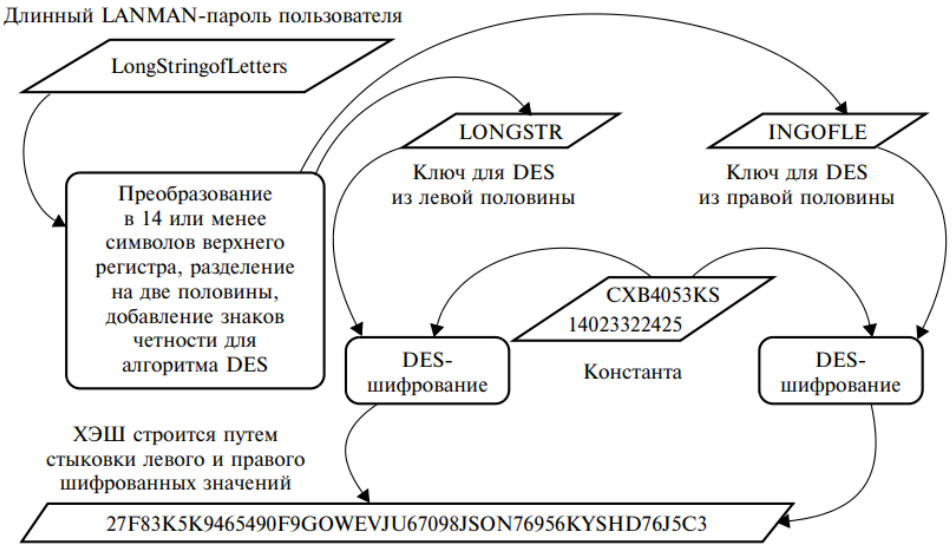

Рисунок 4 – Хеширование LANMAN

В NTLM разработчики ОС Windows NT существенно улучшили механизм аутентификации по сравнению с LANMAN. В NT сохраняется 14-символьное хеширование на длину пароля, но можно пользоваться любыми символами Unicode. Пароли сохраняются и хранятся в последовательности из четырнадцати 16-битовых Unicode-символов. Для получения 128-разрядного хеша используется алгоритм MD4 (тоже небезопасный ныне). В NTLMv2 разработчики стали использовать алгоритм MD5.

В целом уязвимости данной схемы можно привести ниже:

- возможность подмены сервера (его аутентичность не проверяется никак);
- подмена пакетов аутентификации (если не включена подпись).

1.1.3.2 Kerberos

Протокол Kerberos был разработан для надежной аутентификации пользователей. Реализуется механизм Single Sign-On (возможности одноразовой аутентификации в нескольких приложениях). Протокол Kerberos обеспечивает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними с учетом того, что надежный обмен информацией между клиентом и сервером может происходить в незащищенной среде, а передаваемые пакеты — перехвачены и модифицированы.

Kerberos использует разные типы сообщений. Наиболее интересны следующие:

1. KRB_AS_REQ: используется для запроса TGT в KDC.
2. KRB_AS_REP: используется для доставки TGT с помощью KDC.
3. KRB_TGS_REQ: используется для запроса TGS в KDC, используя TGT.
4. KRB_TGS_REP: используется для доставки TGS с помощью KDC.
5. KRB_AP_REQ: используется для аутентификации пользователя в отношении службы с использованием TGS.
6. KRB_AP_REP: (Необязательно) Используется службой для идентификации себя по отношению к пользователю.
7. KRB_ERROR: Сообщение для сообщения об ошибках.

Типы соответствуют этапам (кроме KRB_ERROR). Этапы аутентификации приведены на Рисунок 5.

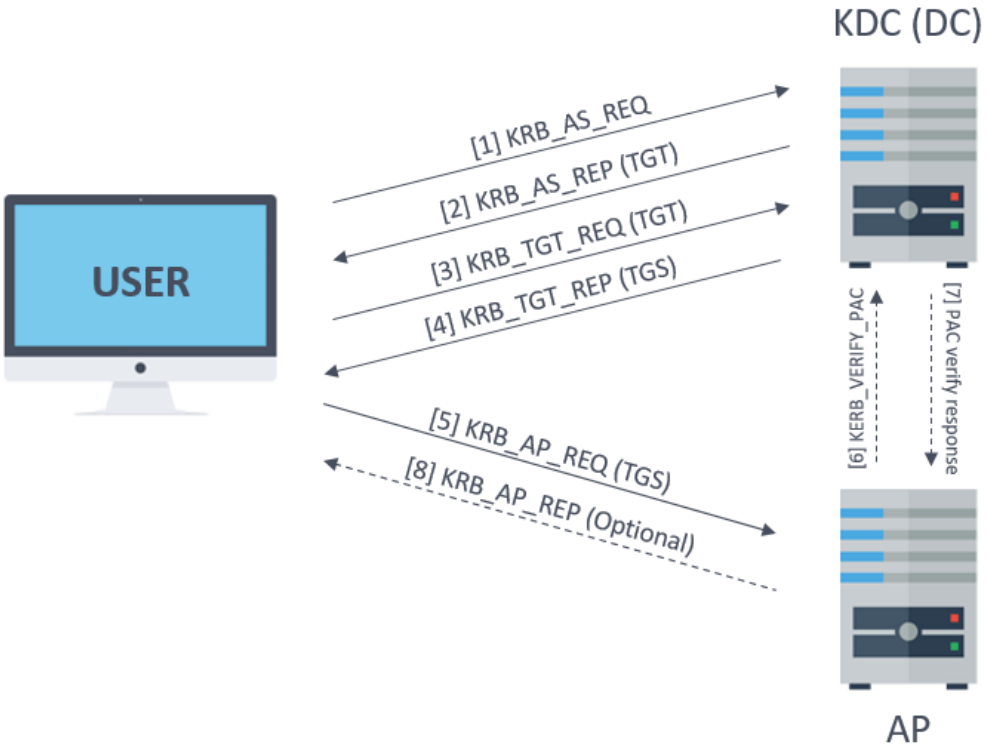

Рисунок 5 – Этапы аутентификации Kerberos

1.1.3.2.1 AS_REQ

Сначала пользователь должен получить TGT от KDC. Для этого необходимо отправить KRB_AS_REQ (Рисунок 6). KRB_AS_REQ имеет следующие поля:

1. Зашифрованная временная метка с клиентским ключом для аутентификации пользователя и предотвращения атак повторного воспроизведения
2. Имя пользователя аутентифицированного пользователя
3. SPN службы, связанный с учетной записью krbtgt
4. Одноразовый номер, созданный пользователем (nonce)

Примечание: зашифрованная временная метка необходима только в том случае, если пользователю требуется предварительная аутентификация, что является обычным явлением, кроме случаев, когда в учетной записи пользователя установлен флаг DONT_REQ_PREAUTH.

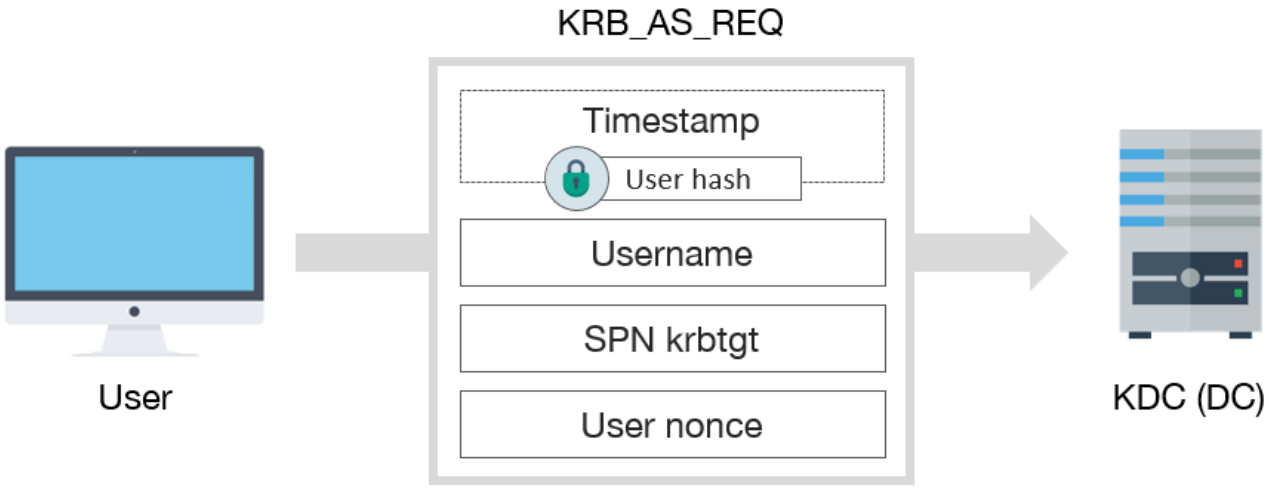

Рисунок 6 – AS_REQ

1.1.3.2.2 AS_REP

После получения запроса KDC проверяет личность пользователя, расшифровывая временную метку. Если сообщение правильное, оно должно ответить KRB_AS_REP (Рисунок 7). KRB_AS_REP включает следующую информацию:

1. Имя пользователя
2. TGT, в который входят:
    a. Имя пользователя
    b. Сессионный ключ
    c. Срок годности TGT
    d. PAC с правами пользователя, подписанный KDC
3. Некоторые зашифрованные данные с помощью пользовательского ключа, в том числе:
    a. Ключ сеанса
    b. Срок годности TGT
    c. Nonce

После завершения у пользователя уже есть TGT, который можно использовать для запроса TGS, а затем доступа к сервисам.

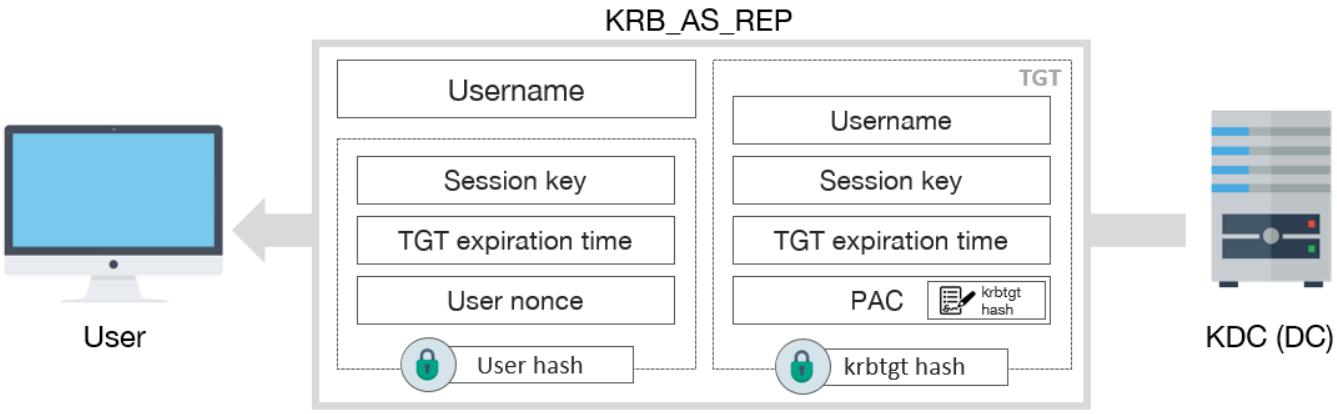

Рисунок 7 – AS_REP

1.1.3.2.3 TGS_REQ

Чтобы запросить TGS, сообщение KRB_TGS_REQ должно быть отправлено в KDC (Рисунок 8). KRB_TGS_REQ включает:

1. Зашифрованные данные с помощью сеансового ключа:
   a. Имя пользователя
   b. Отметка времени
2. TGT
3. SPN запрашиваемой услуги
4. Nonce

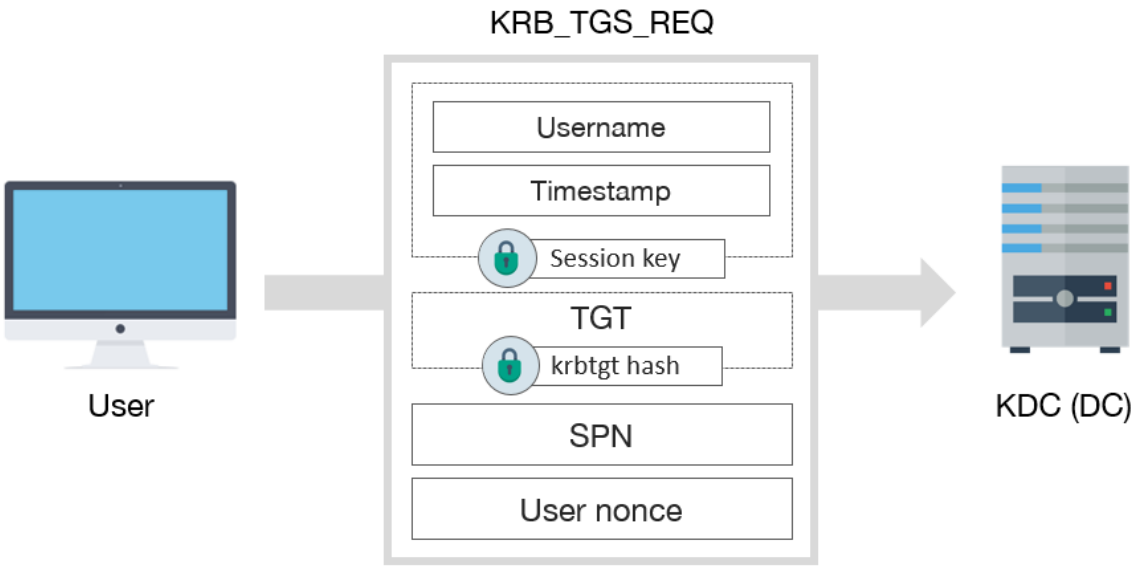

Рисунок 8 – TGS_REQ

1.1.3.2.4 TGS_REP

После получения сообщения KRB_TGS_REQ KDC возвращает TGS внутри KRB_TGS_REP (Рисунок 9). KRB_TGS_REP включает:

1. Имя пользователя
2. TGS, который содержит:
    a. Ключ сеанса обслуживания
    b. Имя пользователя
    c. Срок годности TGS

d. PAC с правами пользователя, подписанный KDC

e. Зашифрованные данные с помощью сеансового ключа:

f. Ключ сеанса обслуживания

g. Срок годности TGS

h. Nonce

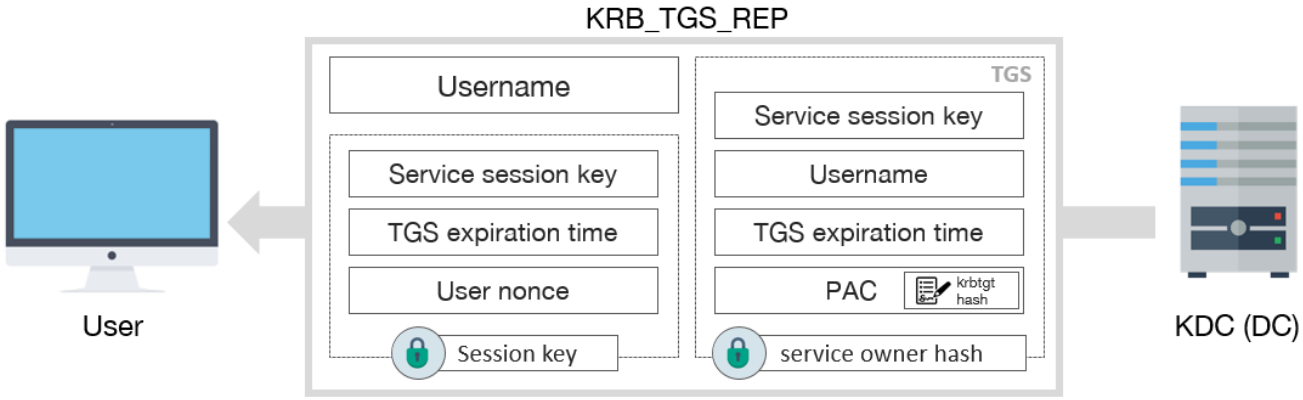

Рисунок 9 – TGS_REP

1.1.3.2.5 AP_REQ

По завершению предыдущего этапа у пользователя уже есть действующий TGS для взаимодействия со службой. Чтобы использовать его, пользователь должен отправить AP сообщение KRB_AP_REQ (Рисунок 10).

KRB_AP_REQ включает:

1. TGS

2. Зашифрованные данные с помощью служебного сеансового ключа:
    a. Имя пользователя
    b. Nonce

После этого, если у пользователя есть права, он может получить доступ к сервису. Если это так, что обычно не происходит, AP проверит PAC по KDC. А также, если требуется взаимная аутентификация, он ответит пользователю сообщением KRB_AP_REP.

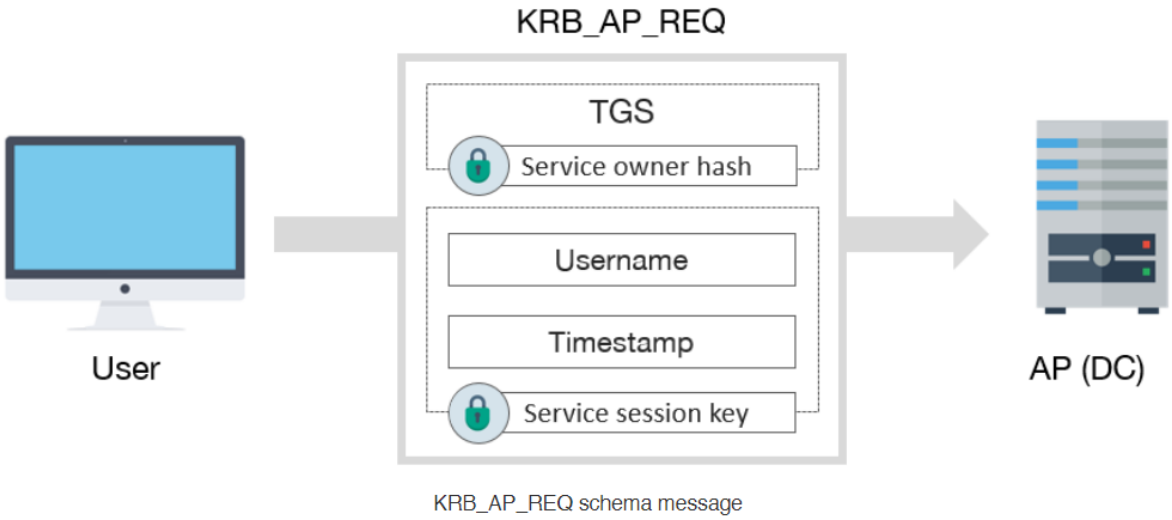

Рисунок 10 – AP_REQ

2 ПРАКТИЧЕСКАЯ ЧАСТЬ

Индивидуальное задание:

1. Получить образы Windows Server 2016 с ролью контроллера домена и Windows 10 и настроить в соответствии с инструкцией.
2. **Переименовать** «Имя компьютера» в Windows 10 по типу «**ФамилияИмя**» на английском языке без пробелов (в Интернете много статей по запросу в Google по типу «how to rename PC in Active Directory Domain») и «Имя пользователя» user1 в «**ФамилияИмя**» на английском языке без пробелов (или создать нового пользователя домена – принципиальной разницы с точки зрения задания нет; как это делать тоже много статей, потребуется поработать с контроллером домена и политиками).
3. Подготовить возможность записи трафика перед включением ОС Windows 10, настроить фильтры ip.addr == <адрес сервера> || ip.addr == <адрес клиента>.
4. Произвести запись трафика (1) при аутентификации клиента в системе.
5. «Экспортировать указанные пакеты» с опцией Displayed в PCAP-файл с записью трафика (1).
6. Произвести запись трафика (2) при запросе asktgt клиента в системе с помощью утилиты Rubeus.
7. «Экспортировать указанные пакеты» с опцией Displayed в PCAP-файл с записью трафика (2).
8. В отчете отразить основные этапы данных запросов на аутентификацию со скриншотами; при этом, чтобы в первых пакетах установления соединения **было видно имя комьютера**, которое является *индивидуальным*:
    a. Запрос AS_REQ (показать зашифрованный timestamp на скрине).
    b. Если есть ошибка PreAuth, то ее тоже нужно обязательно показать на скриншоте.
    c. Ответ AS_REP (показать полученный TGT).
    d. Запрос TGS_REQ (только для трафика (1), показать полученный TGT).
    e. Ответ TGS_REP (только для трафика (1), показать полученные TGT и TGS).

f. Словами ответить на вопрос: в чем принципиальное отличие легитимного запроса TGT и запроса TGT с помощью Rubeus в данном задании (п. 2.2).

9. Произвести запись трафика (3) при запросе setspn клиента с именем клиентской Windows 10.
10. «Экспортировать указанные пакеты» с опцией Displayed в PCAP-файл с записью трафика (3).
11. В отчете отразить этапы:
    a. Найти запрос на выгрузку списка SPN-записей.
    b. Найти место в трафике, где будет приведен список SPN-записей в ответе сервера.

2.1 Подготовительная часть

Для проведения лабораторной работы потребуются следующие ВМ и ПО:

1. Windows Server 2016 (в качестве гостевой ОС).
2. Windows 10 (в качестве гостевой ОС).
3. Wireshark.

Для развертывания ВМ требуется скачать файл OVA и импортировать конфигурацию через главное окно VirtualBox (Рисунок 11).

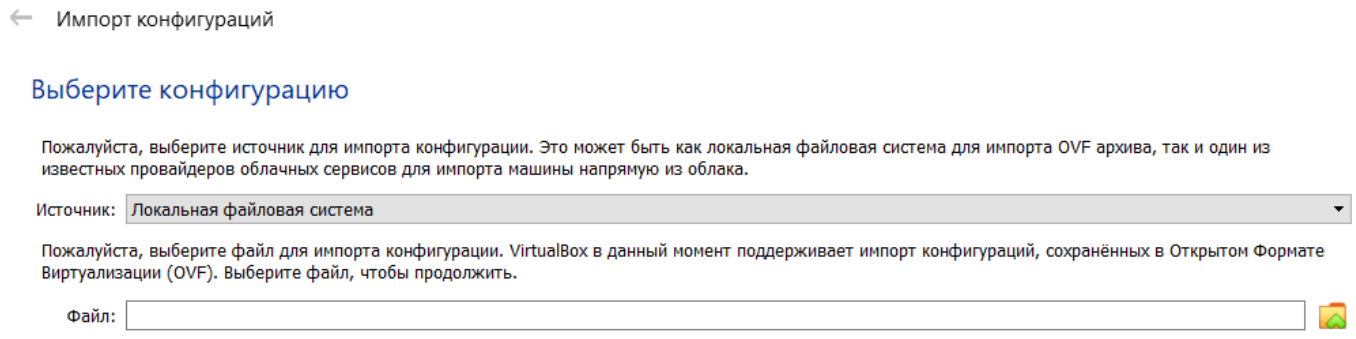

Рисунок 11 – Импорт конфигураций ВМ

После импорта конфигурации рекомендуется выключить ВМ и сделать Snapshot стабильного образа ВМ.

2.2 Проведение эксперимента

2.2.1 Проведение эксперимента для трафика (1) и (2)

Для записи трафика (1) достаточно зайти в систему с учетными данными user1:1234. Доменный админ имеет следующие учетные данные domadmin:1234

Для записи трафика (2) в Windows 10 открыть командную строку (Win + R), запустить:

cd Documents

Rubeus asktgt /user:user1 /password:1234 /ptt

Данная команда позволит запустить Rubeus с запросом TGT-тикета.

2.2.2 Проведение эксперимента для трафика (3)

Для записи трафика (3) в Windows 10 открыть командную строку (Win + R), запустить:

setspn –L <имя хоста>

2.3 Задание на максимальную оценку

Выполнение всех пунктов задания подразумевает максимальную оценку 8 баллов. На получение оценок 9 и 10 могут претендовать те, кто сделает все обязательные задания без ошибок и смогут продемонстрировать на скриншоте (а там должно быть в командной строке индивидуальное имя пользователя из индивидуального задания) способ получения билетов при помощи утилиты mimikatz со всеми этапами в отчете. При этом нужно указать (хотя бы кратко по каждому этапу): что делает та или иная команда утилиты.

3 ЗАКЛЮЧЕНИЕ

В рамках данной работы получены знания:

– об Active Directory;

– об аутентификации в Active Directory.

В рамках данной работы получены навыки:

– сравнения легитимной аутентификации и запроса билетов с помощью утилиты Rubeus;

– анализа дампов трафика с запросом типов служб SPN.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149 // Российская бизнес-газета. – 2006 – № 4131.

2. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем; введ. 01.04.2016 – М.: Федеральное агентство по техническому регулированию и метрологии, 2016. – 12 с.