вМИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»
КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ
ПРЕПОДАВАТЕЛЬ

Профессор, д.т.н.		Н. Н. Мошак
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1

Настройка локальных политик безопасности АРМ

по курсу: БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. № 5712		Д.И. Коваленко
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2020

1. Цель работы

Цель работы – изучить и научиться настраивать локальные политики безопасности на автономном автоматизированном рабочем месте (АРМ) пользователя с установленной на нем операционной системой (ОС) Windows для защиты информации от несанкционированного доступа (НСД).

Используемое программное обеспечение: ОС версии не ниже WindowsXP. А именно Windows 7 Professional (x64).

Тип ИС закрытого контура: 1Г**.**

2. Теоретические сведения

Основные угрозы нарушения конфиденциальности ресурсов АРМ - это компрометация ключевой информации систем криптографической защиты информации и несанкционированное предоставление привилегий пользователям в ОС Windows АРМ.

Основные угрозы нарушения целостности программ и данных АРМ – это несанкционированное изменение операционной среды АРМ; действия нарушителя в среде ИС от имени легального пользователя, носящие деструктивный характер или приводящие к искажению информации.

Основные угрозы нарушения доступности активов АРМ – изменения конфигурации ОС (файлов CONFIG.SYS и AUTOEXEC.BAT, файлов ядра ОС для Windows); удаления (модификации) исполняемых файлов прикладного и системного программного обеспечения; внесения компьютерных вирусов; эксплуатации программ, осуществляющих некорректные действия, из-за имеющихся в них ошибок или специальных «закладок».

Требования по защите АРМ от НСД «закрытого» и «открытого» контура ИС

Подсистема защиты АРМ от НСД «закрытого» и «открытого» контура должна обеспечивать: однозначную идентификацию пользователей в ИС и в операционной системе (далее – ОС) АРМ (использование общих идентификаторов (ни в СЗИ, ни в ОС) не допускается; идентификацию по логическим именам информационных ресурсов (логических устройств, каталогов, файлов).

Управление доступом в АРМ должна базироваться на стандартных механизмах идентификации, аутентификации и разграничения доступа предоставляемых:

1. *BIOS ПЭВМ;*
2. *сертифицированным программно-аппаратным комплексом защиты от НСД СЗИ;*

3. *ОС Windows АРМ;*
4. *сетевой ОС;*
5. *СУБД;*
6. *средствами усиленной аутентификации ACE Server (SecurID) или Kerberos.*

Завершение работы пользователем АРМ должно сопровождаться освобождением всех занимаемых им разделяемых ресурсов (Logout).

Все входящие носители информации должны проверяться на наличие вирусов.

АРМ «закрытого» и «открытого» контура ИС должны защищаться от НСД с помощью сертифицированной системы защиты информации (СЗИ) от НСД. Настройка системы защиты от НСД на каждом АРМ осуществляется индивидуально, с учетом решаемых на этом АРМ задач, при этом, независимо от используемой операционной системы на АРМ, у пользователя не должно быть возможности запускать собственные, не разрешенные явно администратором безопасности, задачи.

В минимальной конфигурации СЗИ от НСД, устанавливаемые на АРМ пользователей, должны обеспечивать:

1. создание изолированной (замкнутой) программной среды (ИПС) на АРМ, обеспечивающей возможность запуска только заданного набора программ и/или процессов. Создание ИПС на АРМ пользователя предполагает настройку СЗИ от НСД и/или средств реестра ОС Winows в режиме, обеспечивающем запуск только технологического программного обеспечения и запрет выполнения программ, не предусмотренных технологическим процессом. Управление ИПС АРМ должно осуществляться централизованно;
2. идентификацию и аутентификацию пользователей, предоставление доступа к ресурсам компьютера только по предъявлению личного аппаратного идентификатора и дополнительным вводом пароля с клавиатуры;
3. контроль ***целостности*** программных средств СЗИ от НСД до входа пользователя в операционную систему;
4. разграничение доступа к локальным каталогам и файлам рабочей станции, обеспечивающее защиту от модификации системного и прикладного программного обеспечения АРМ;
5. регистрацию попыток входа в систему и попыток доступа к важнейшим объектам локальной файловой системы компьютера;
6. блокировку работы пользователей в случае нарушения ограничений, наложенных СЗИ от НСД.

Кроме того, настройка СЗИ от НСД должна запрещать пользователю выполнение следующих действий согласно приведенной табл. 2.1.

Таблица 2.1

Наименование запрета	Пояснения
Запрет загрузки с внешних носителей	Пользователю запрещается осуществлять загрузку компьютера с системной дискеты или с загрузочного CD ROM диска
Запрет работы при нарушении целостности	При обнаружении факта нарушения целостности контролируемых файлов доступ пользователя к компьютеру блокируется.
Запрет работы при изъятии аппаратной поддержки	При обнаружении факта изъятия устройства аппаратной поддержки из компьютера доступ пользователя к компьютеру блокируется. При попытке пользователя войти в систему на экран будет выведено предупреждающее сообщение, и загрузка компьютера будет прервана
Запрет работы при изменении конфигурации	При обнаружении факта изменения конфигурации компьютера, доступ пользователя к компьютеру блокируется. При попытке пользователя войти в систему на экран выводится предупреждающее сообщение, и загрузка компьютера прерывается.
Запрет доступа к портам	Пользователю запрещается обмен информацией через коммуникационные порты компьютера.
Запрет на редактирование системного реестра	Пользователю запрещается изменять параметры системного реестра.
Запрет изменения настроек сети	Пользователю запрещено изменение параметров работы сетевой карточки, сетевых протоколов и других настроек «сетевого окружения» в операционной системе
Запрет изменения параметров безопасности	Пользователю запрещен доступ к изменению политик безопасности.
Запрет выполнения функций, не определенных технологическим процессом	Пользователю запрещено выполнять программное обеспечение, не используемое в технологическом процессе

Локальные политики безопасности АРМ – это набор параметров безопасности операционной системы Windows и системы защиты информации от НСД, которые

обеспечивают безопасность АРМ в соответствии с требованиями политики информационной безопасности ИС организации. Для настройки локальной политики безопасности на автономном АРМ используется оснастка «Локальная политика безопасности». Если АРМ входит в состав домена, изменение политик, привязанных к домену ActiveDirectory, можно настраивать при помощи оснастки «Редактор управления групповыми политиками».

3. Ход выполнения работы

Для настройки локальной политики безопасности на автономном АРМ используется оснастка «Локальная политика безопасности».

3.1. Подготовка к настройке локальных политик безопасности

3.1.1. Установка макета варианта лабораторной работы на диске C.

Была проведена установка макета на диске G, а именно VirtualBox с ОС Windows.

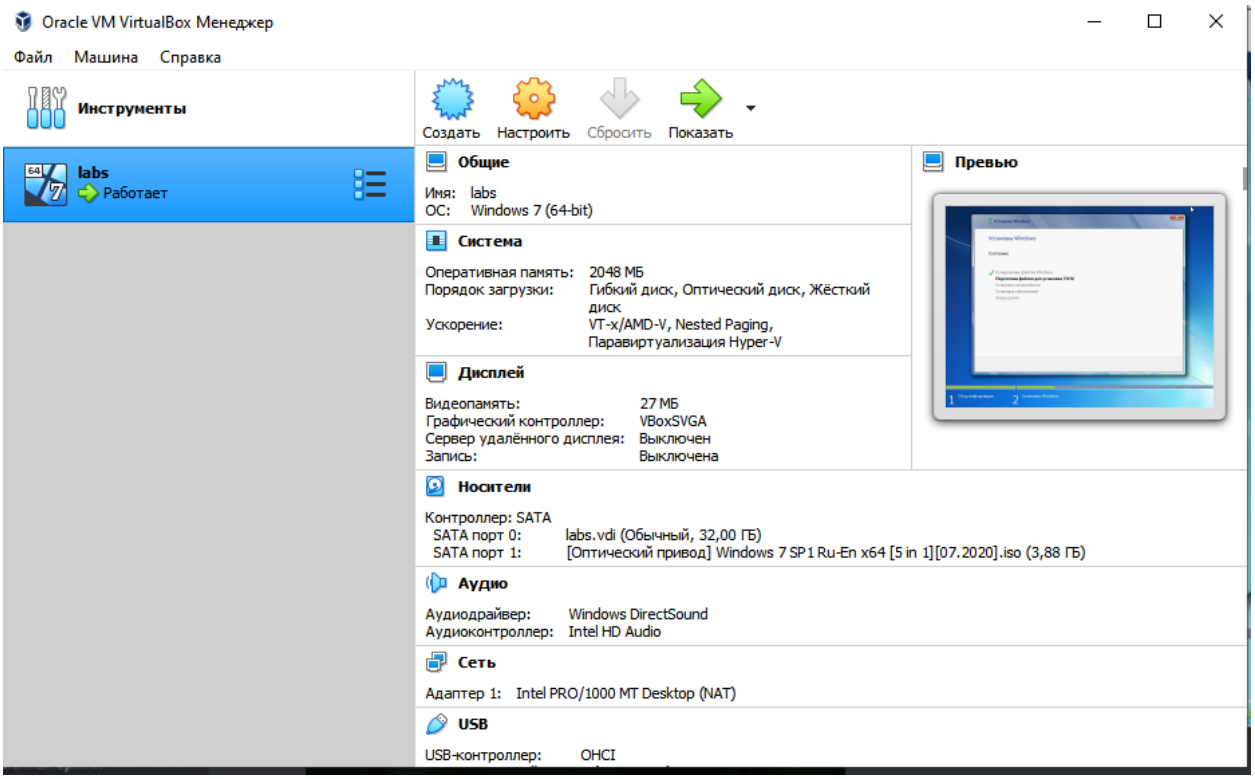


Рисунок 1 - Запуск ОС на ВМ

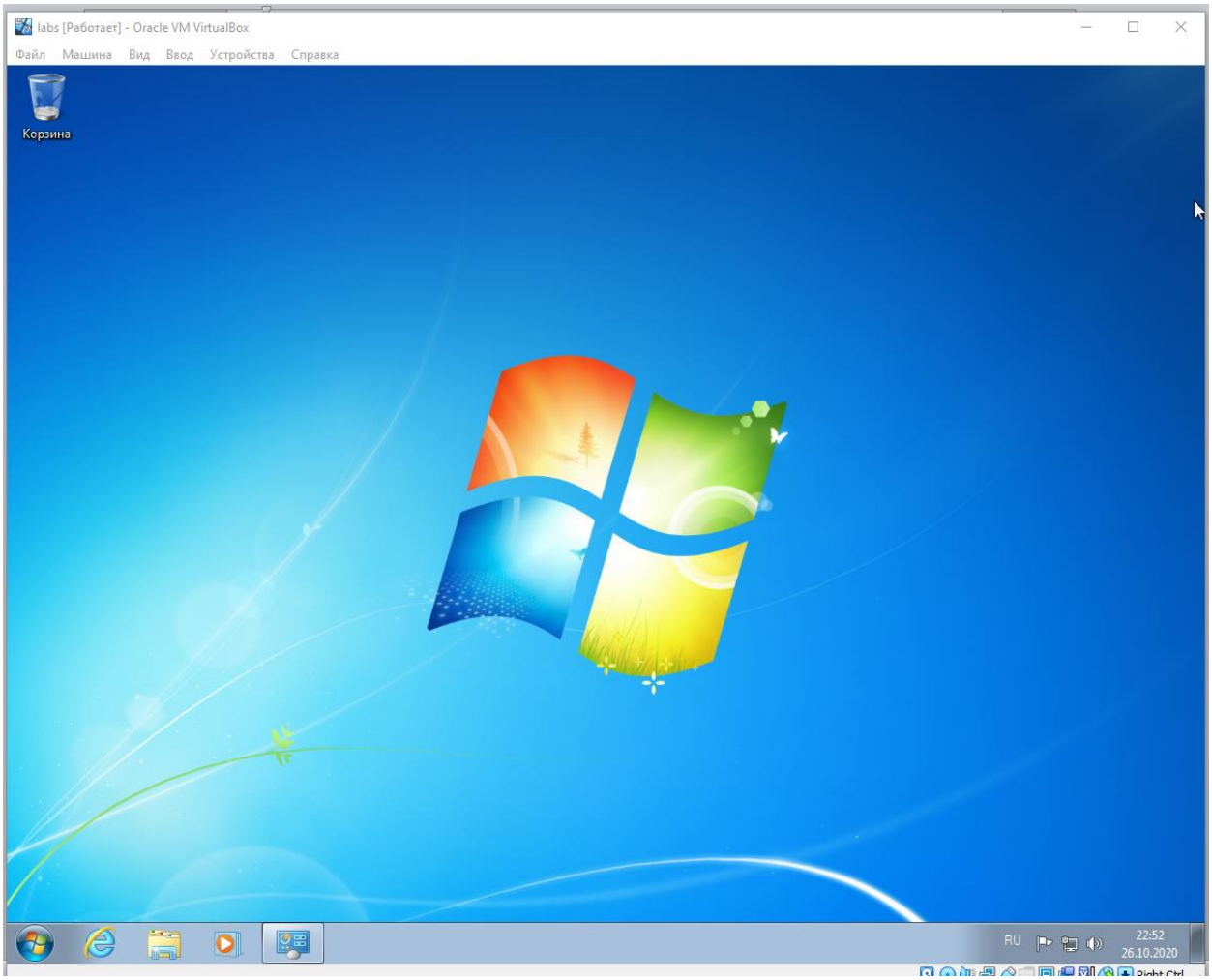


Рисунок 2 - Работающая ОС на ВМ

3.1.2. Переход к настройке локальных политик безопасности.

Переходим к настройкам локальных политик безопасности через поиск. Вводим «Локальная политика безопасности», и открываем приложение.

3.2. Управление встроенными учетными записями

Для защиты ИС от НСД используется разграничение доступом, которое заключается в предоставлении пользователям прав, зависящие от из учетных записей.

В данном примере будет рассмотрена гостевая учетная запись. Здесь запись имеет множество ограничений, благодаря которым у гостя не будет возможности получить доступ к данным и изменениям настроек.

По умолчанию гостевая учетная запись выключена, поэтому надо включить ее. Для этого переходим по следующему пути: Пуск →Локальная политика безопасности (Поиск) → Параметры безопасности → Локальные политики → Параметры безопасности → Учетные записи: Состояние учетной записи «Гость» и активировать её, как показано на Рисунке 3.

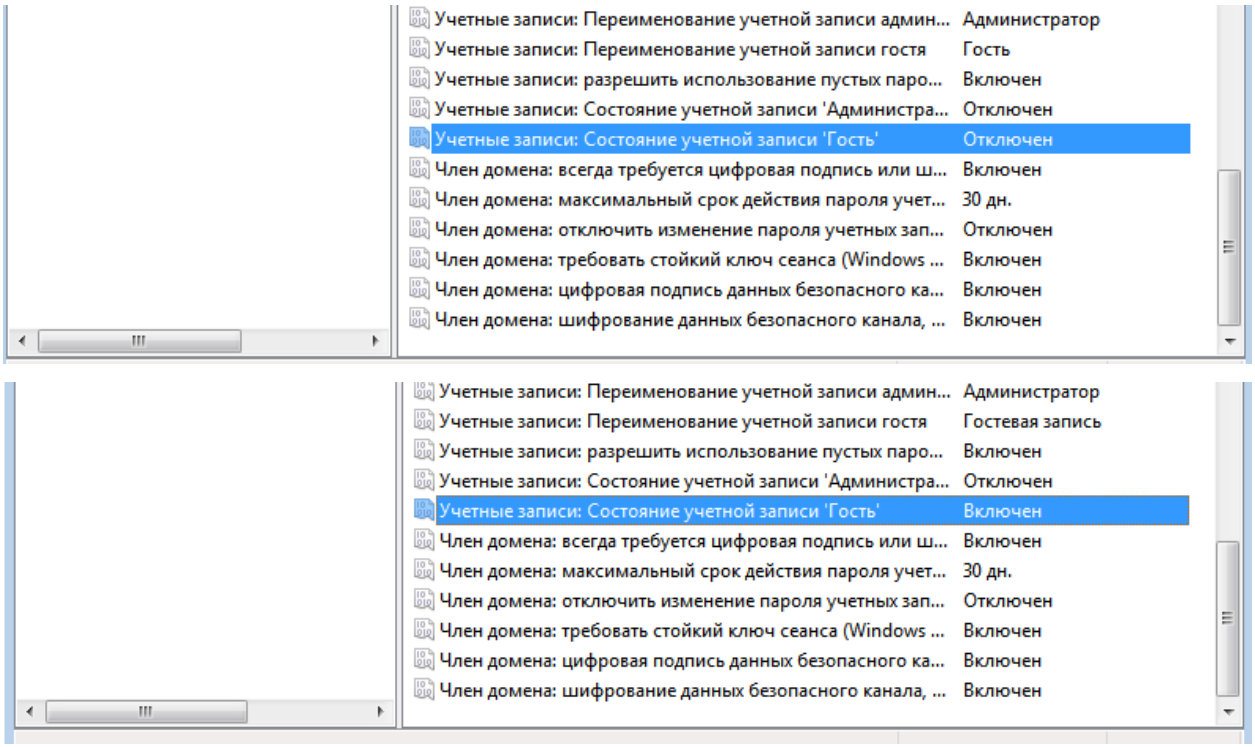


Рисунок 3 - Включение гостевой учетной записи

Название «Гость» иногда усложняет жизнь администратора. В реальных случаях у нас может быть не один пользователь, да и конкретика в именах играет тоже роль в обеспечении безопасности.

Для переименования гостевой учетной записи нужно открыть: Пуск →Локальная политика безопасности (Поиск) → Параметры безопасности → Локальные политики → Параметры безопасности → Учётные записи: Переименование учетной записи гостя, как показано на Рисунке 4, после чего нужно перезагрузить компьютер.

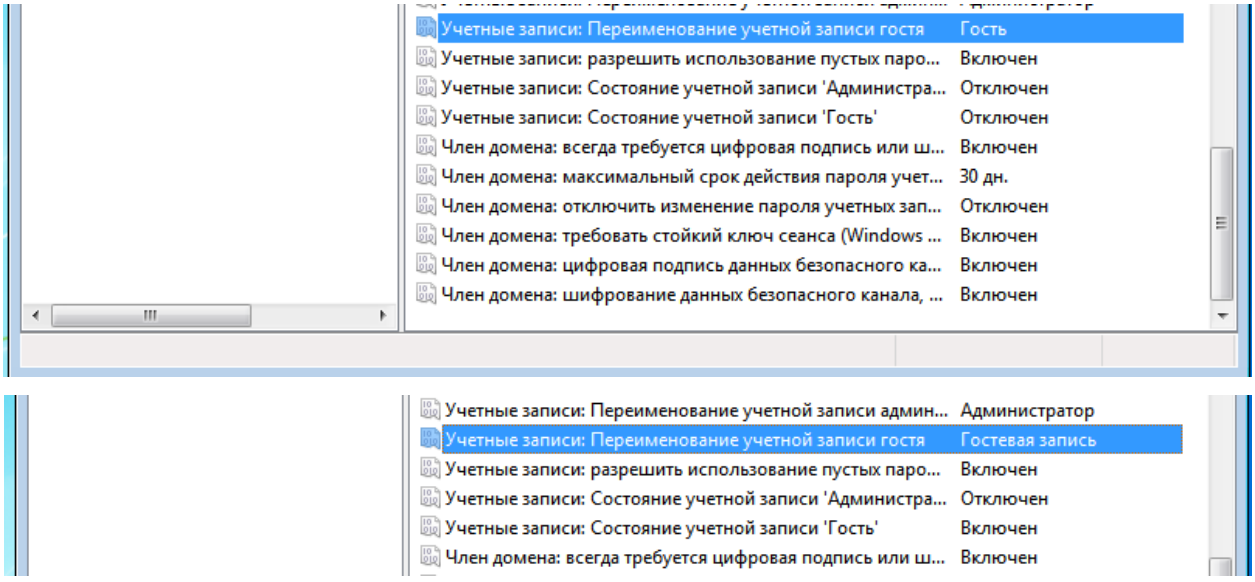


Рисунок 4 - Переименование гостевой учетной записи

После перезагрузки компьютера проверяем, применилась ли политика безопасности к вашему компьютеру. Открываем в панели управления компонент «Учетные записи пользователей» и переходим по ссылке «Управление другой учетной записью». В открывшемся окне можно увидеть все учетные записи, созданные на локальном компьютере, в том числе переименованную учетную запись гостя. Все показано на Рисунке 5.

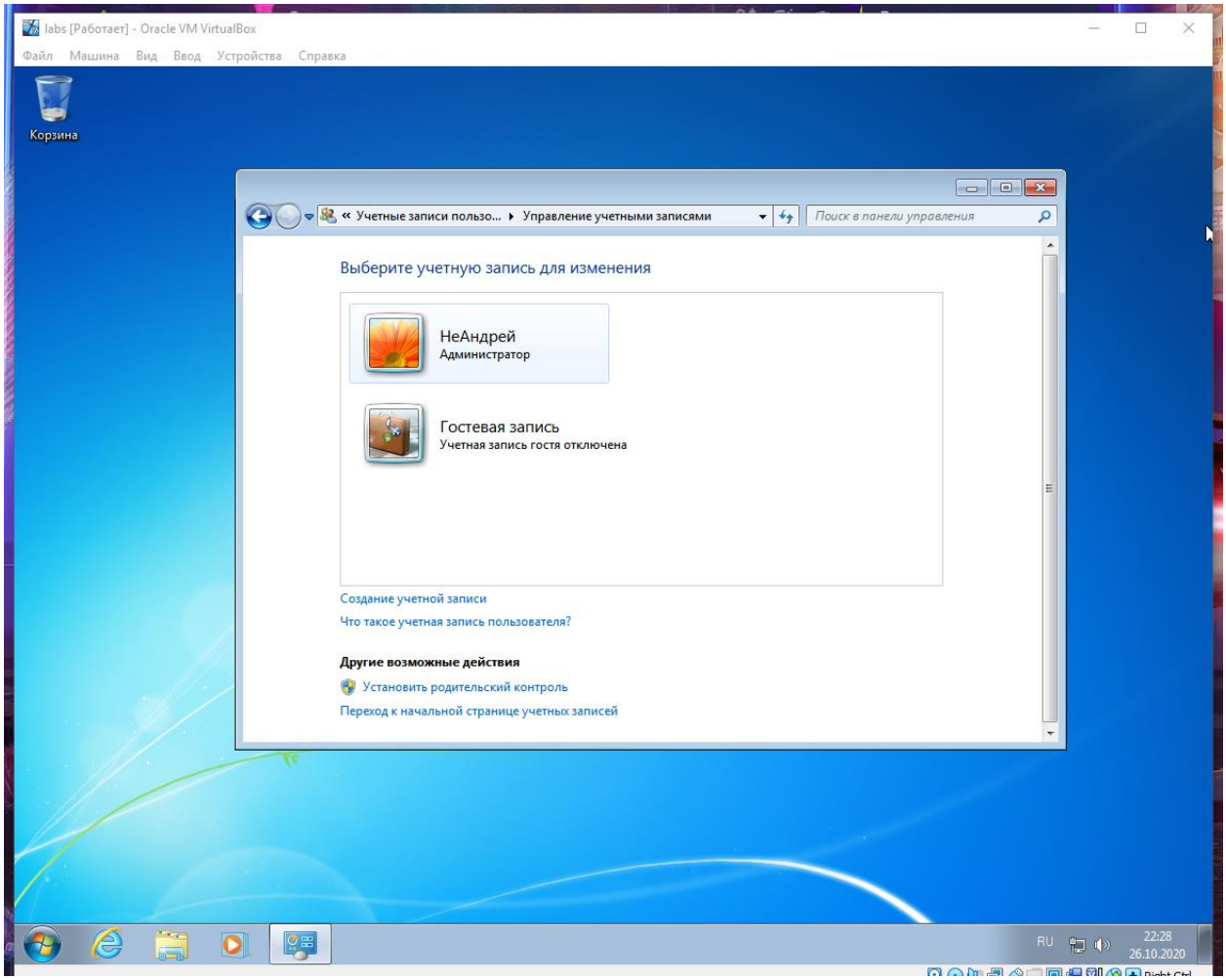


Рисунок 5 - Результат переименования гостевой учетной записи

3.3. Управление политиками паролей

Следующим инструментом РД при работе на АРМ является установка паролей учётных записей. Надёжность использования паролей, а соответственно подсистемы РД, является правильная настройка «Политики паролей» – совокупности правил, накладывающих разумные ограничения на пользовательские пароли. К таким правилам относятся:

1. ***Максимальные срок действия пароля, т.е. период времени, в течение которого пользователь обязан изменить пароль для продолжения работы на АРМ. Доступные значения могут быть установлены в промежутке от 0 до 999 дней. Однако для обеспечения своевременной сменяемости пароля,***

рекомендуется выбирать максимальный срок действия от 14 до 30 суток, именно за такой срок, в худшем случае, возможен подбор пароля.

2. ***Минимальная длина пароля. Значение данной политики сравнивается с длиной устанавливаемого пароля и запрещает его использование, в случае если его длина меньше указанной. Рекомендуемое значение от 8 до 16 символов.***
3. ***Минимальные срок действия пароля, т.е. период времени, в течение которого изменение пароля невозможно. Следует отметить, что значение данной политики не должно превышать максимального срока действия пароля.***
4. ***Требование неповторяемости паролей, т.е. политика, устанавливающая ограничение на установку «старого» пароля в качестве «нового». Значение политики – количество старых паролей, с которыми происходит сравнение при выборе нового. Должна обеспечивать «обновляемость» паролей и согласовываться со сроками смены паролей. Таким образом, при смене паролей каждые 15 суток, хранение квартальной базы (6 прежних паролей) оптимально.***
5. ***Хранение паролей, используя обратимое шифрование. Использование данной политики рекомендуется исключительно в тех случаях, когда используются приложения, требующие пароль для аутентификации пользователя. 6. Пароль должен отвечать требованиям сложности. Данная политика устанавливает ограничение на характеристики пароля и предотвращает использование «простых» паролей, существенно повышая уровень безопасности, в следствии чего обязательна к использованию. К вносимым ограничениям относятся:***

a. использование букв верхнего и нижнего регистра одновременно;

b. использование цифр от 0 до 9;

c. использование специальных символов (например, !, @, #, $, *);

d. запрет использования имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

Требование неповторяемости паролей. Указывается количество предыдущих паролей пользователя, с которыми будет сравниваться новый пароль. Зададим этой политике значение 1.

Хранение паролей, используя обратимое шифрование. Для того чтобы пароли невозможно было перехватить при помощи приложений, ActiveDirectory хранит

только хэш-код. Но если перед вами встанет необходимость поддержки приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности, вы можете использовать текущую политику. Обратимое шифрование по умолчанию отключено, так как, используя эту политику, уровень безопасности паролей и всего домена в частности значительно понижается. Использование этой функции аналогично хранению пароля в открытом виде. Оставляем данную политику отключенной.

Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов, на основании руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Данный Руководящий документ разработан в дополнение ГОСТ 34.003-90, ГОСТ 34.601-90, РД 50-680-88, РД 50-34.680-90 и других документов.

Для установки данных требований нужно перейти: Пуск → Локальная политика безопасности (Поиск) → Параметры безопасности → Политики учетных записей → Политика паролей, как показано на Рисунке 6.

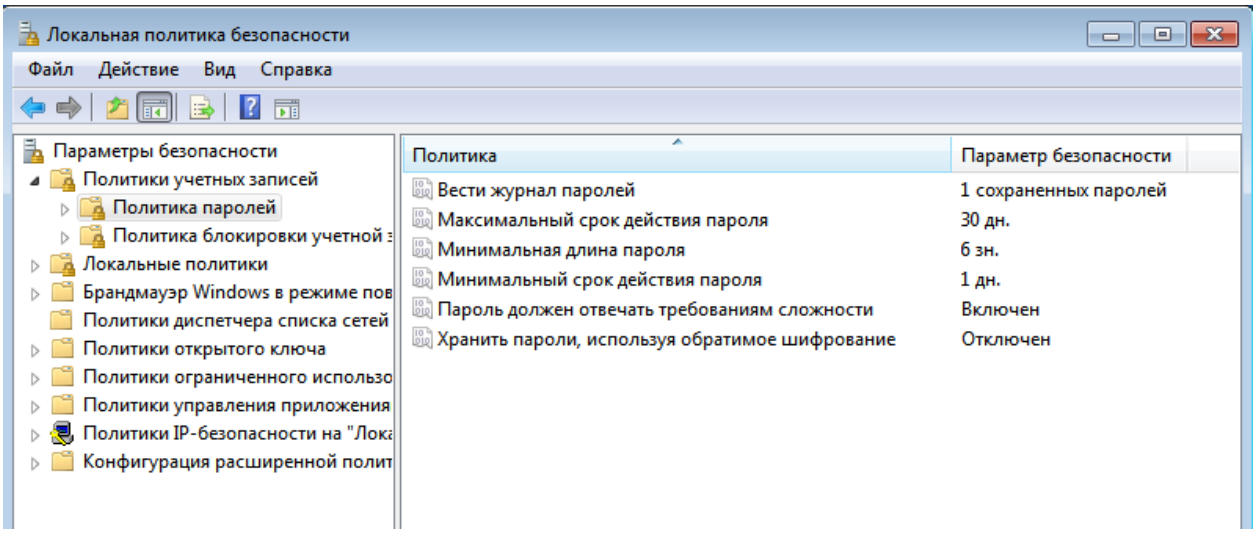


Рисунок 6 - Настроенные политики управлением паролей

3.4. Политика блокировки учетной записи

Даже после создания сложного пароля и правильной настройки политик безопасности, учетные записи ваших пользователей все еще могут быть подвергнуты атакам недоброжелателей.

Политики безопасности Windows могут противостоять таким действиям, используя набор политик узла *«Политика блокировки учетной записи»*. При помощи данного набора политик, есть возможность ограничения количества некорректных попыток входа пользователя в систему. Для этого узла доступны только три политики:

1. ***Установить время до сброса счетчиков блокировки. ActiveDirectory и групповые политики позволяют автоматически разблокировать учетную запись, количество попыток входа в которую превышает установленное вами пороговое значение. При помощи этой политики устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки. Было взято значение равное 30 минут. Это значение должно быть меньше значения политики «Продолжительность блокировки учетной записи». Было взято значение равное 1 минуте.***

2. ***Установить пороговое значение блокировки. Используя эту политику, вы можете указать количество некорректных попыток входа, после чего учетная запись будет заблокирована. Окончание периода блокировки учетной записи задается политикой «Продолжительность блокировки учетной записи» или администратор может разблокировать учетную запись вручную. Количество неудачных попыток входа может варьироваться от 0 до 999. Это значение было установлено равным 5, так как если человек и ошибся, то у него была бы возможность ввести верно данный, не прибегая к помощи администратора.***

3. ***Установить продолжительность блокировки учетной записи. При помощи этого параметра вы можете указать время, в течение которого учетная запись будет заблокирована до ее автоматической разблокировки. Вы можете установить значение от 0 до 99999 минут. В том случае, если значение этой политики будет равно 0, учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее вручную. В случае блокировки учетной записи в связи не верно введенным паролем пять раз, продолжительность блокировки была выставлена 60 минут, чтобы можно было выявить на какой машине произошла блокировка.***

Для изменения «Политика блокировки учетной записи» необходимо перейти по пути: Пуск → Локальная политика безопасности (Поиск) → Параметры безопасности → Политики учетных записей → Политика блокировки учетной записи. Действие показаны на рисунке 7.

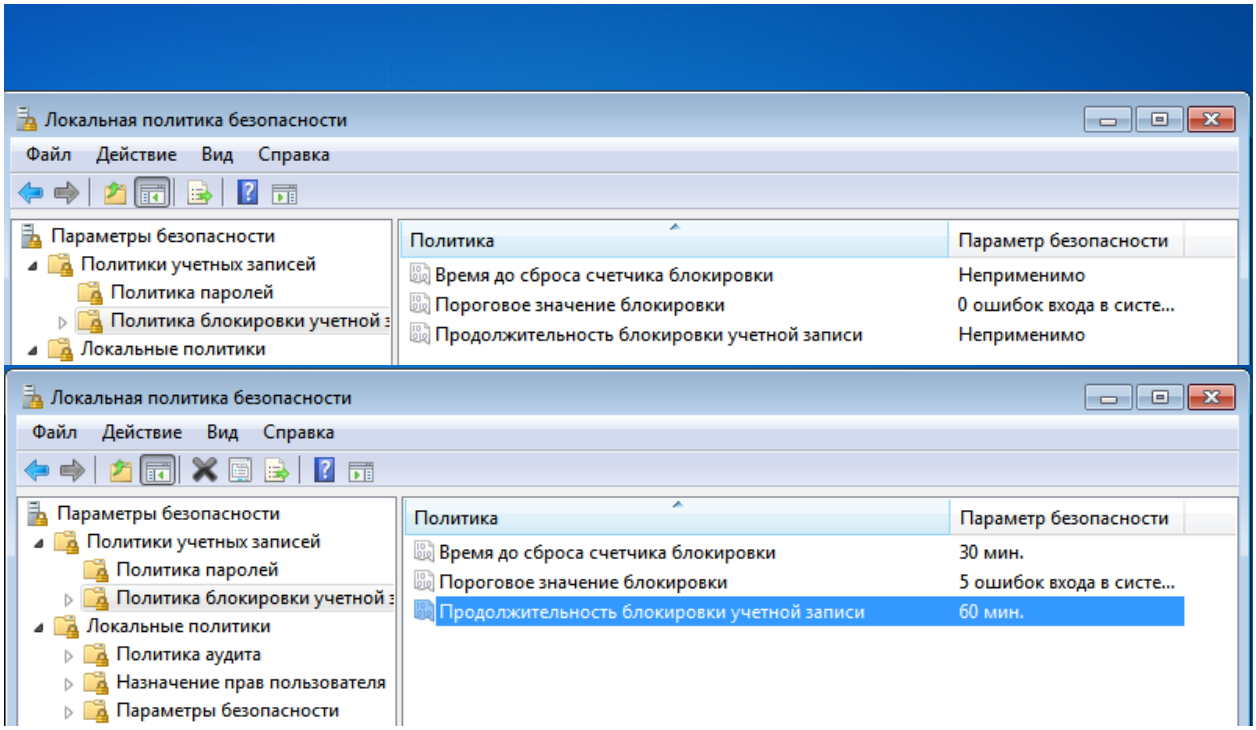


Рисунок 7 - Настройки «Политики блокировки учетных записей»

3.5. Политика аудита

Аудит – процесс, проводимый с целью совершенствования используемых мер по обеспечению ИБ на каком-либо объекте информатизации и состоящий в сборе подробной сводки информации обо всех попытках вторжения и случаях неудачной аутентификации пользователей, а также в проведении подробного анализа собранной информации. В свою очередь, политика аудита – есть совокупность параметров, определяющих какая информация будет поступать в журнал аудита АРМ.

Политика аудита включает следующие параметры:

1. ***Аудит входа в систему. Политика, определяющая будет ли событие входа пользователя в систему заноситься в журнал аудита. Аудит успешных событий определяет порядок фиксации успешных входов (выходов) в систему (из системы), аудит отказов определяет тот же порядок для противоположных событий. 9 В случае настройки политики аудита в АРМ с «открытым контуром» использование аудита успеха не целесообразно, в виду обработки общедоступной информации, в случае АРМ с «закрытым» контуром, ситуация противоположна. В соответствии с п. 2.1. требованиям к АРМ категории 1Г, необходимо вести подробный учёт пользователей, как получивших доступ к защищаемой информации, так и тех, кому в доступе было отказано.***

2. ***Аудит доступа к объектам. Политика, определяющая аудит попыток доступа пользователей к объектам, задаваемым собственными списками в системном***

списке управления доступом (SACL), а также при условии соответствия мандата пользователя грифу объекта. Как и для «аудита входа в систему», целесообразно использование аудитов отказа. Как и при настройке аудита, выбор сведений, подлежащих учёту и контролю, зависит от циркулируемой информации. В случае «закрытого» контура проведение такого учёта – обязательно, в соответствии с п. 2.1.5 требованиям к АРМ категории 1Г.

3. Аудит доступа к службе каталогов. Политика, определяющая порядок аудита событий, указанных в SACL, который можно редактировать в диалоговом окне «Дополнительные параметры безопасности» свойств объекта ActiveDirectory. Аудит происходит только для событий, указанных в SACL, а также при условии соответствия мандата пользователя грифу объекта. Для ИС «открытого» контура наиболее целесообразно применение политики аудита отказов, с другой стороны, для ИС «закрытого» контура является обязательным производить учёт доступа любых пользователей к защищаемым сведениям, в соответствии с п. 2.1.3 и 2.1.5 требованиям к АРМ категории 1Г, поэтому также необходимо использование аудита успехов.

4. Аудит изменения политики. Политика, указывающая будет ли ОС фиксировать попытки изменения политики назначения прав пользователям, аудита, учетной записи или доверия Так как несанкционированное изменение политики может повлечь за собой повышение прав доступа пользователей, вплоть до доступа к конфиденциальной информации, а также изменению политик безопасности для любых ИС обязательным требованием является выполнения аудита не только отказов, но и успехов.

5. Аудит изменения привилегий. Политика, определяющая будет ли выполняться аудит использования привилегий и прав пользователей. Как и в случае «аудита изменения политики», несанкционированное изменение привилегий может стать угрозой ИБ системы, поэтому целесообразно использование аудита как успехов, так и отказов.

6. Аудит отслеживания процессов. Данная политика определяет, порядок аудита событий, связанных с процессами (создание и завершение процессов, активация программ и непрямой доступ к объектам). В виду общедоступности обрабатываемой информации (для АРМ «открытого» контура), проведение аудита успехов нецелесообразен, в отличие от аудита отказов. В тоже время, для систем «закрытого» контура, необходимо производить учёт любых событий, связанных с процессами, с целью обеспечения учёта доступа пользователей (программы,

пользовательских процессов) к защищаемой информации, в соответствии с п. 2.1 требованиям к АРМ категории 1Г.

7. Аудит системных событий. Данная политика определяет, порядок аудита системных событий, таких как перезагрузка ПК, факты сбоя системы аудита, внесение изменений, способных повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени. В виду важности системных событий целесообразен аудит как успеха, так и отказа, вне зависимости от степени конфиденциальности обрабатываемой информации.

8. Аудит событий входа в систему. Политика, определяющая порядок выполнения аудита каждый раз при проверке данным компьютером учетных данных, как при локальном, так и удаленном входе пользователя в систему, при удаленном подключении к общей папке. Проведение аудита успехов обязательно только для АРМ «закрытого» контура, в соответствии с п. 2.1.1 требованиям к АРМ категории 1Г, в отличие от аудита отказов, проведение которого важно с точки зрения совершенствование СЗИ любой системы.

9. Аудит управления учетными записями. Политика, определяющая порядок выполнения аудита событий управления учетными записями на компьютере (создание, перемещение и отключение учетных записей, изменение паролей и групп). В виду того, что данная политика играет важную роль в совершенствовании организации ИБ, а также требованиям руководящего документа, целесообразно ведение аудита как успехов, так и отказов, вне зависимости от степени защищаемой информации.

Аудит, рассмотренных событий, по умолчанию не проводится, для изменения параметров политики аудита необходимо перейти по пути: Пуск → Локальная политика безопасности (Поиск) → Параметры безопасности → Локальные политики → Политики аудита и выбрать оптимальный режим и полноту аудита. Требования по аудиту к АС первой группы, а именно класса 1Г предполагает следующие параметры безопасности:

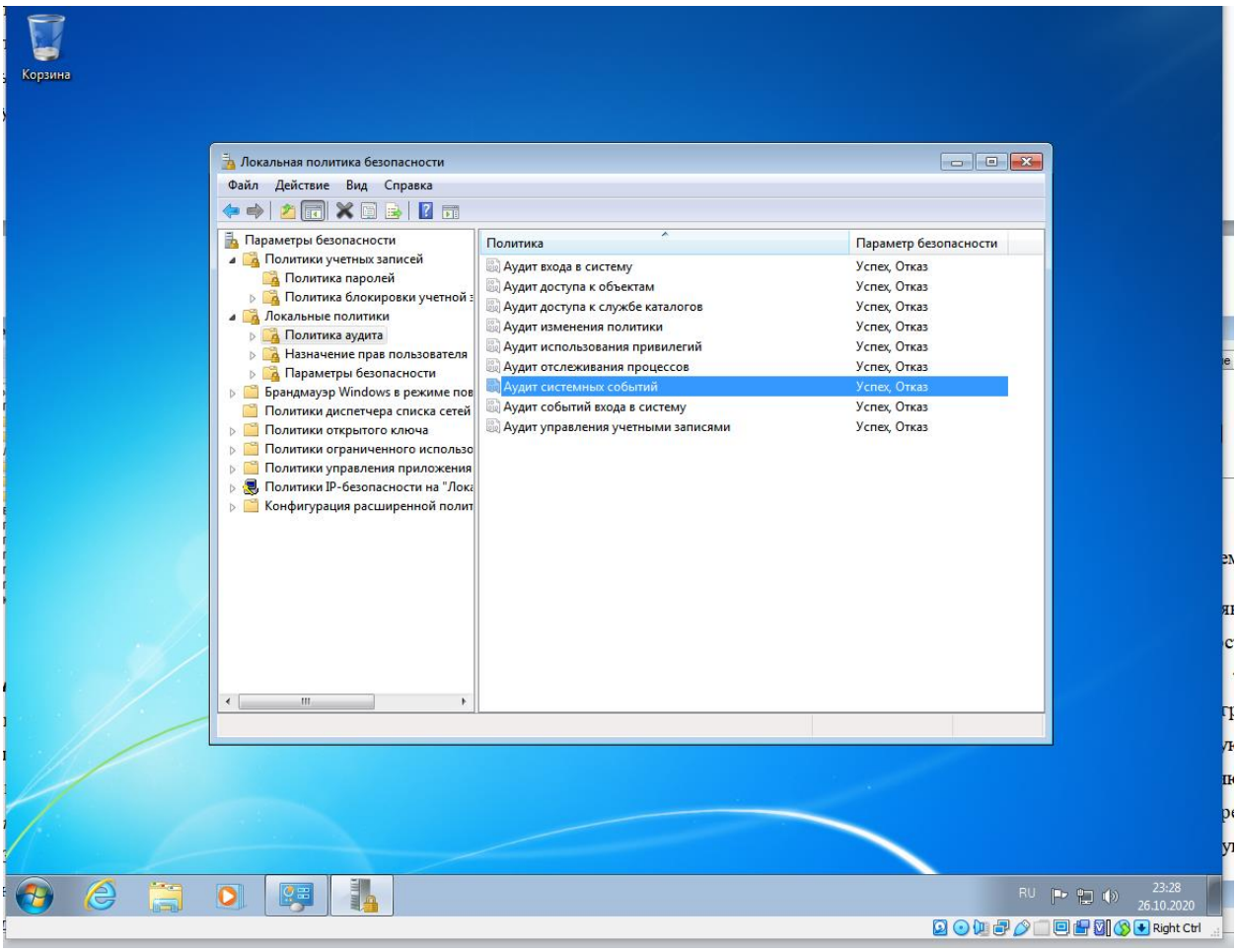


Рисунок 8 - Настройка «Политика аудита» по умолчанию

3.6. Политика назначения прав пользователей

Угрозы информационной безопасности могут быть не только внешними, но и внутренними, т.е. ослабление защищенности могут быть вызваны некорректными действиями легальных пользователей, как в следствии злого умысла, так и недостаточной квалификацией. С целью предупреждения внутренних угроз целесообразно разумно ограничивать права и привилегии пользователей и групп пользователей. Для назначения прав доступны 44 политики безопасности. Рассмотрим некоторые из политик:

1. ***Добавление рабочих станций к домену. Политика, предоставляющая пользователям (или группам пользователей) добавлять компьютеры в домен ActiveDirectory (до 10 компьютеров). Стоит отметить, что по умолчанию все пользователи, прошедшие проверку подлинности, на контроллерах домена могут добавлять до 10 компьютеров, для обеспечения состояния наибольшей защищенности целесообразно назначение данной привилегии исключительно группе администраторов ИС, вне зависимости от обрабатываемой в ИС информации.***

2. ***Доступ к компьютеру из сети. Политика, предоставляющая разрешение подключения к компьютеру по сети указанным пользователям (или группам***

пользователей). На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы» и «Операторы архивации», «Пользователи» и «Все». В целях предотвращения НСД, для любых ИС, целесообразно ограничивать доступ из сети, т.е. не предоставлять доступ группе «Все».

3. Завершение работы системы. Политика, определяющая список пользователей, которые имеют право на использование команды «Завершение работы» после удачного входа в систему. На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы», «Операторы архивации» и «Пользователи» (только на рабочих станциях). Так как порядок завершение работы ОС напрямую влияет на её правильную работоспособность, целесообразно предоставление соответствующих полномочий исключительно администраторам ИС как «закрытого», так и открытого контура.

4. Запрет входа в систему через службу удаленных рабочих столов. Политика, определяющая список пользователей (или групп пользователей), которым запрещён входа в систему в качестве клиента удаленных рабочих столов. По умолчанию, как на рабочих станциях, так и на серверах, всем разрешено входить в систему как клиенту удаленных рабочих столов. Очевидно, что любая учетная запись, которой разрешен вход в систему с помощью служб удаленных рабочих столов, может быть использована для входа в удаленную консоль устройства. Если это право пользователя не ограничивается законными пользователями, которым требуется вход на консоль компьютера, злоумышленник может установить ПО, которое повышает права пользователей, именно поэтому обязателен тщательный отбор пользователей, которым будет предоставлена данная привилегия, вне зависимости от грифа защищаемой информации.

5. Запрет локального входа. Политика, запрещающая отдельным пользователям (или группам пользователей) выполнять вход в систему. По умолчанию всем пользователям разрешен вход в систему. Однако неавторизованные пользователи могут войти на консоль устройства, загрузить и запустить вредоносное ПО, которое повышает права пользователей. Поэтому важно, вне зависимости от грифа информации, циркулирующей в системе, произвести отбор пользователей и установить запрет соответствующей категории.

6. Изменение системного времени. Политика, предоставляющая право изменения системного времени отдельным пользователям (или группам пользователей). Стоит отметить, что данная политика также предоставляет право изменять соответствующее время отслеживаемых событий в Журнале

событий. На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы» и «Локальная служба».

В виду существенного влияния системного времени на состояние защищенности системы, целесообразно предоставить право его изменения исключительно администраторам ИС, как «открытого», так и «закрытого» контуров.

Для изменения политик по умолчанию необходимо перейти по адресу: Пуск → Выполнить → Локальная политика безопасности (Поиск) → Параметры безопасности → Локальные политики → Назначение прав пользователей.

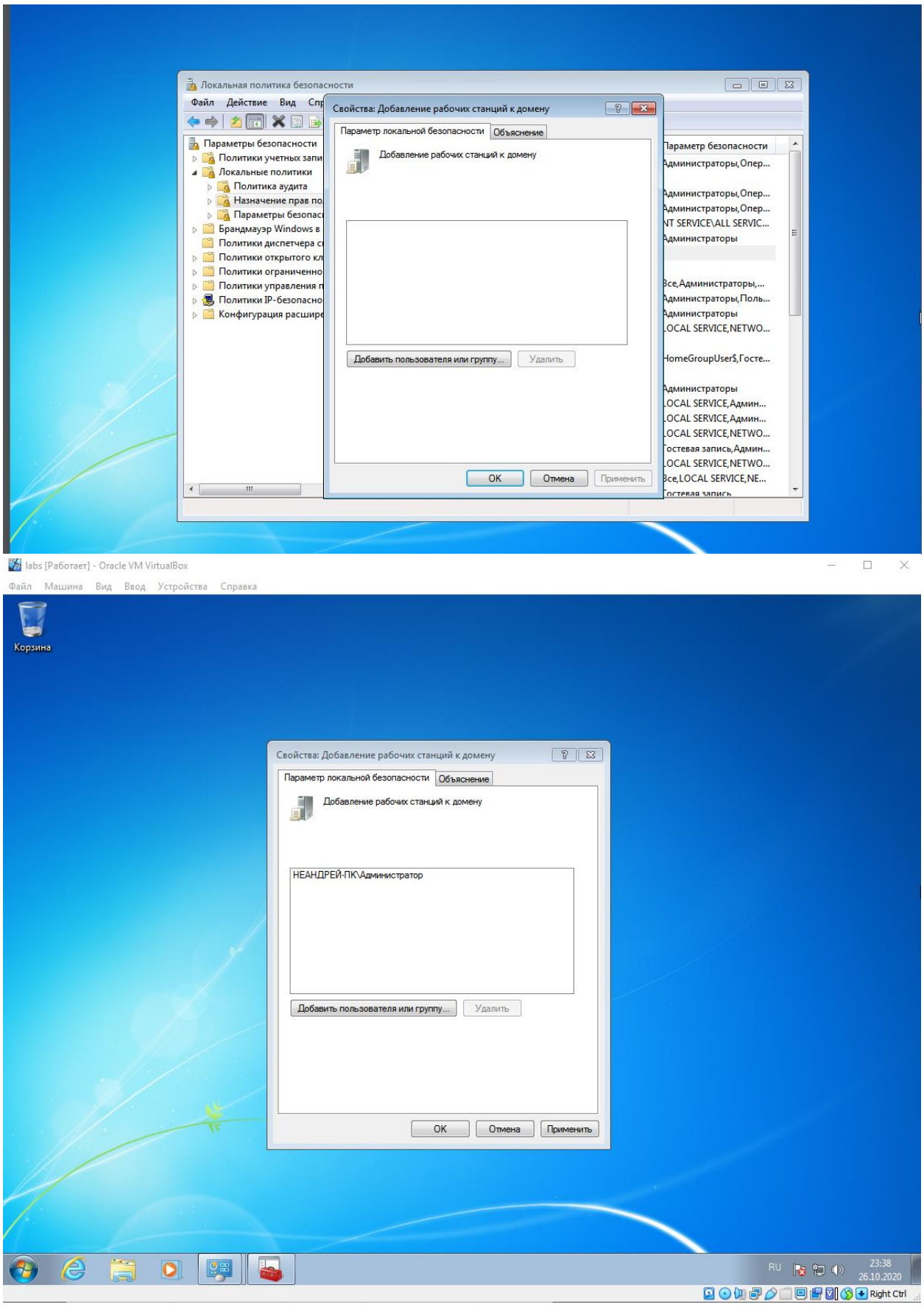


Рисунок 9 - Изменение свойств «Добавление рабочих станций к домену» (Свеху - значение по умолчанию, снизу - пользовательская настройка)

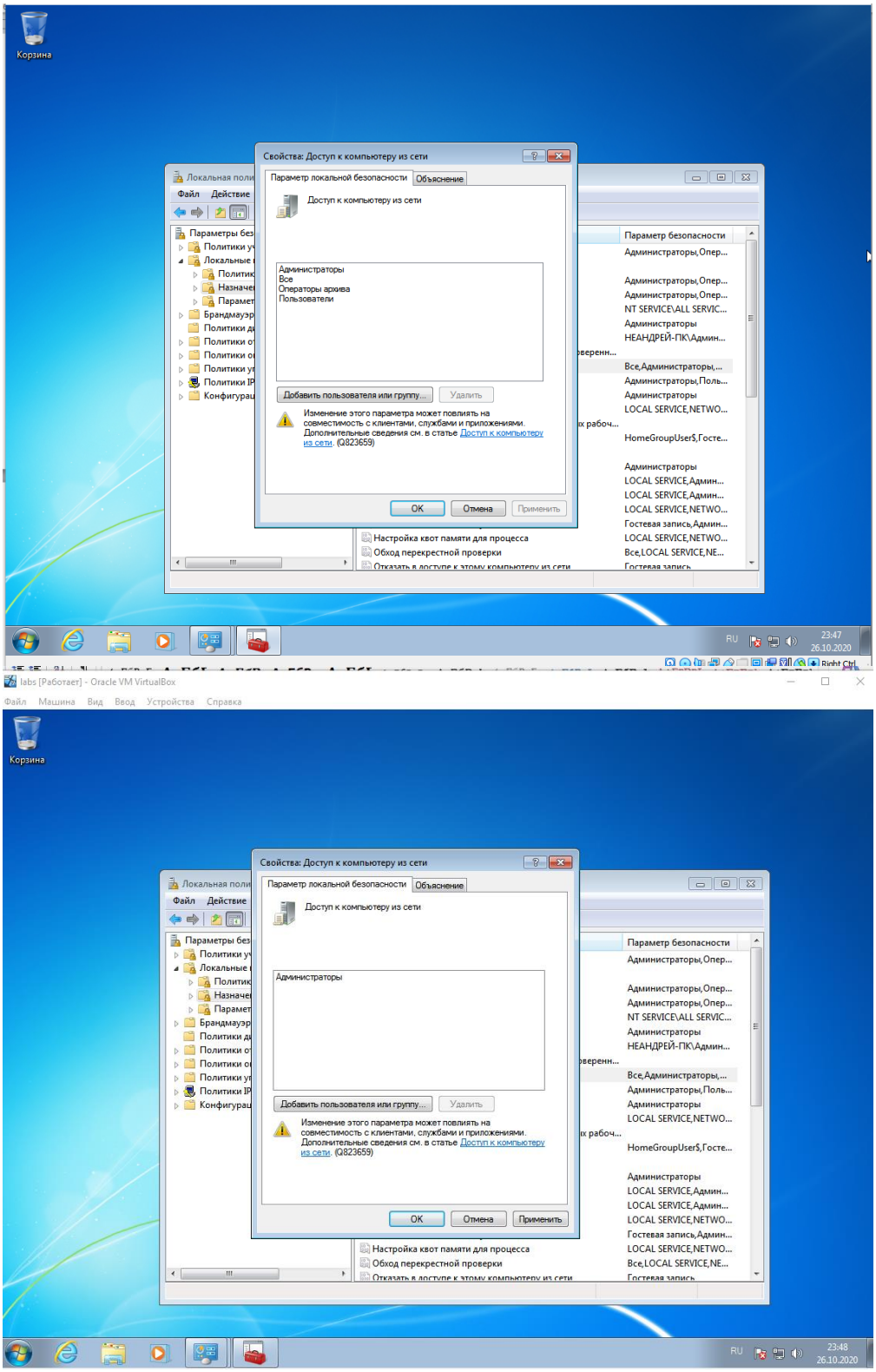


Рисунок 10 - Изменение свойств «Доступ к компьютеру из сети» (Сверху - значение по умолчанию, снизу - пользовательская настройка)

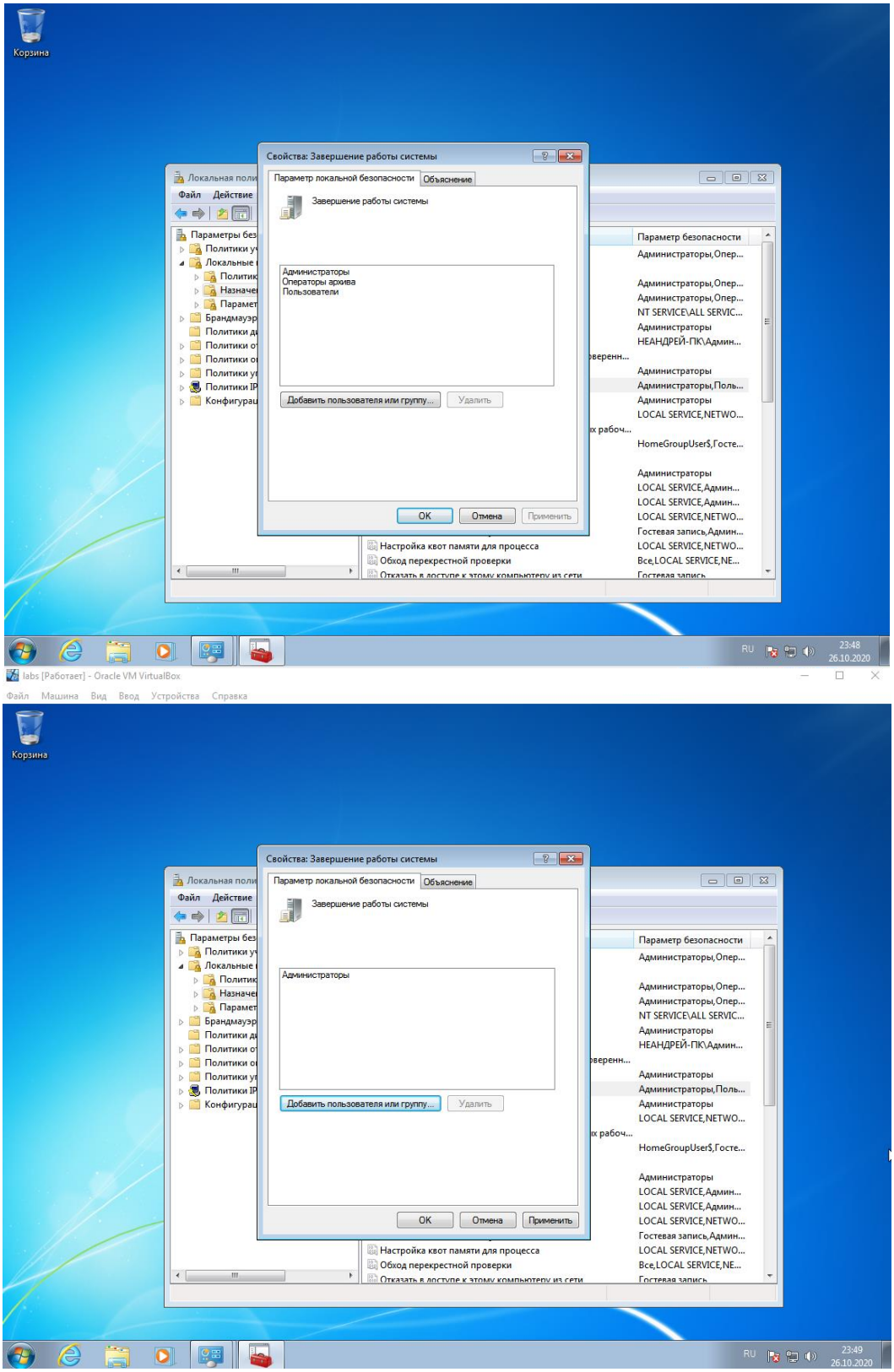


Рисунок 11 - Изменение свойств «Завершение работы системы» (Сверху - значение по умолчанию, снизу - пользовательская настройка)

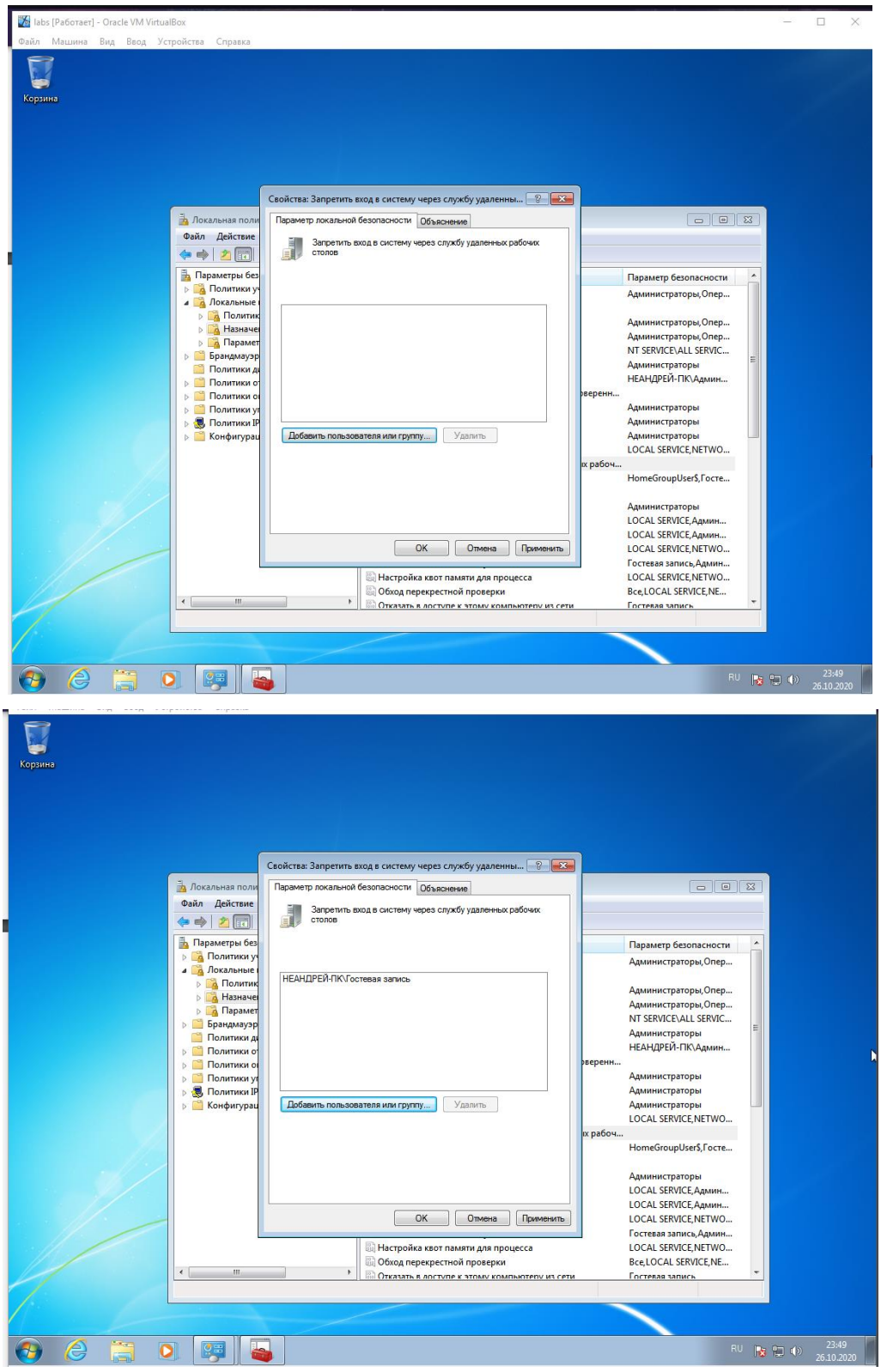
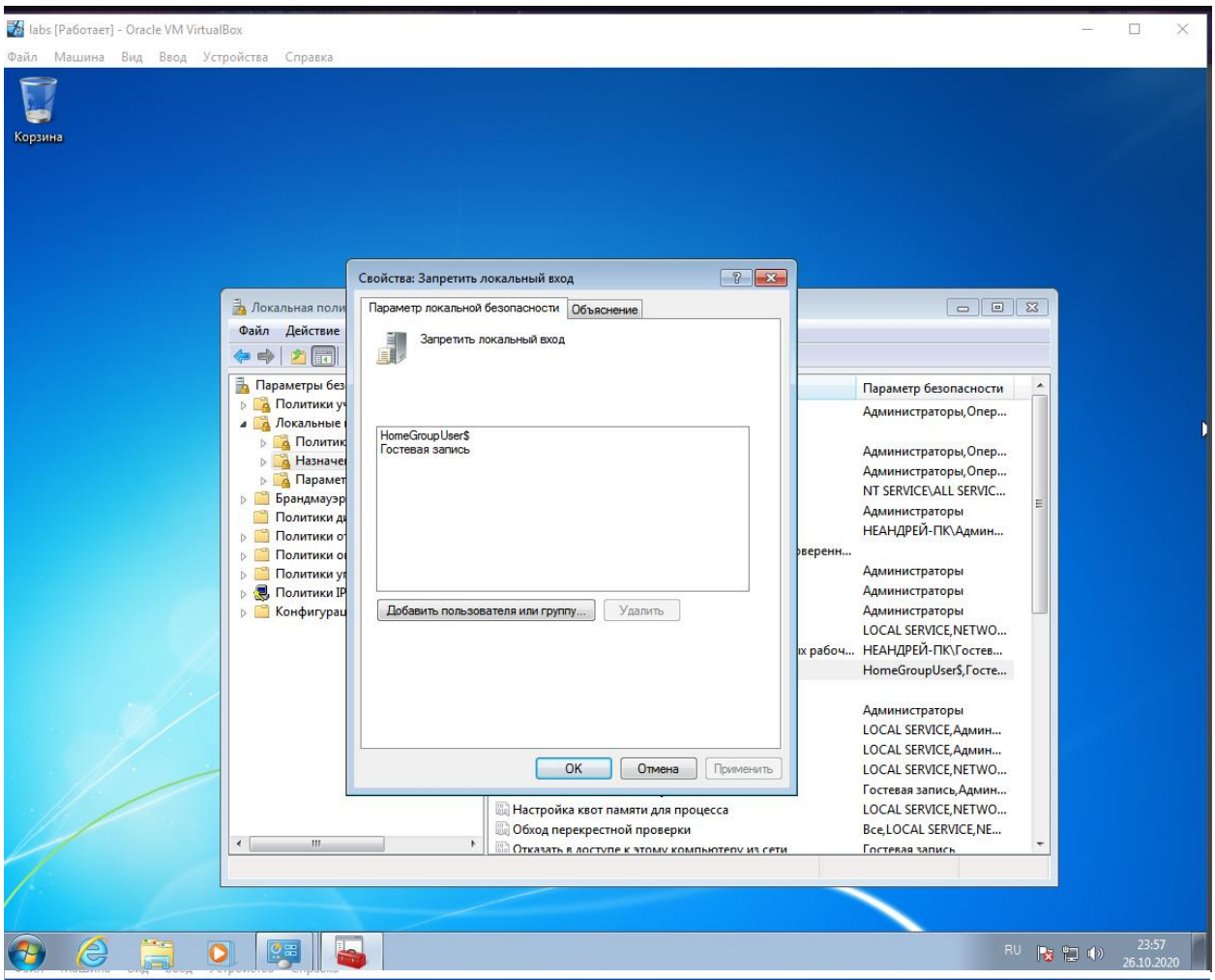


Рисунок 12 - Изменение свойств «Запретить вход в систему через службу удаленных рабочих столов» (Сверху - значение по умолчанию, снизу - пользовательская настройка)


labs [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Корзина
Свойства: Запретить локальный вход
Параметр локальной безопасности
Объяснение
Запретить локальный вход
HomeGroupUser$
Гостевая запись
Добавить пользователя или группу...
Удалить
OK
Отмена
Применить
Параметр безопасности
Настройка квот памяти для процесса
Обход перекрестной проверки
RU
23:57
26.10.2020

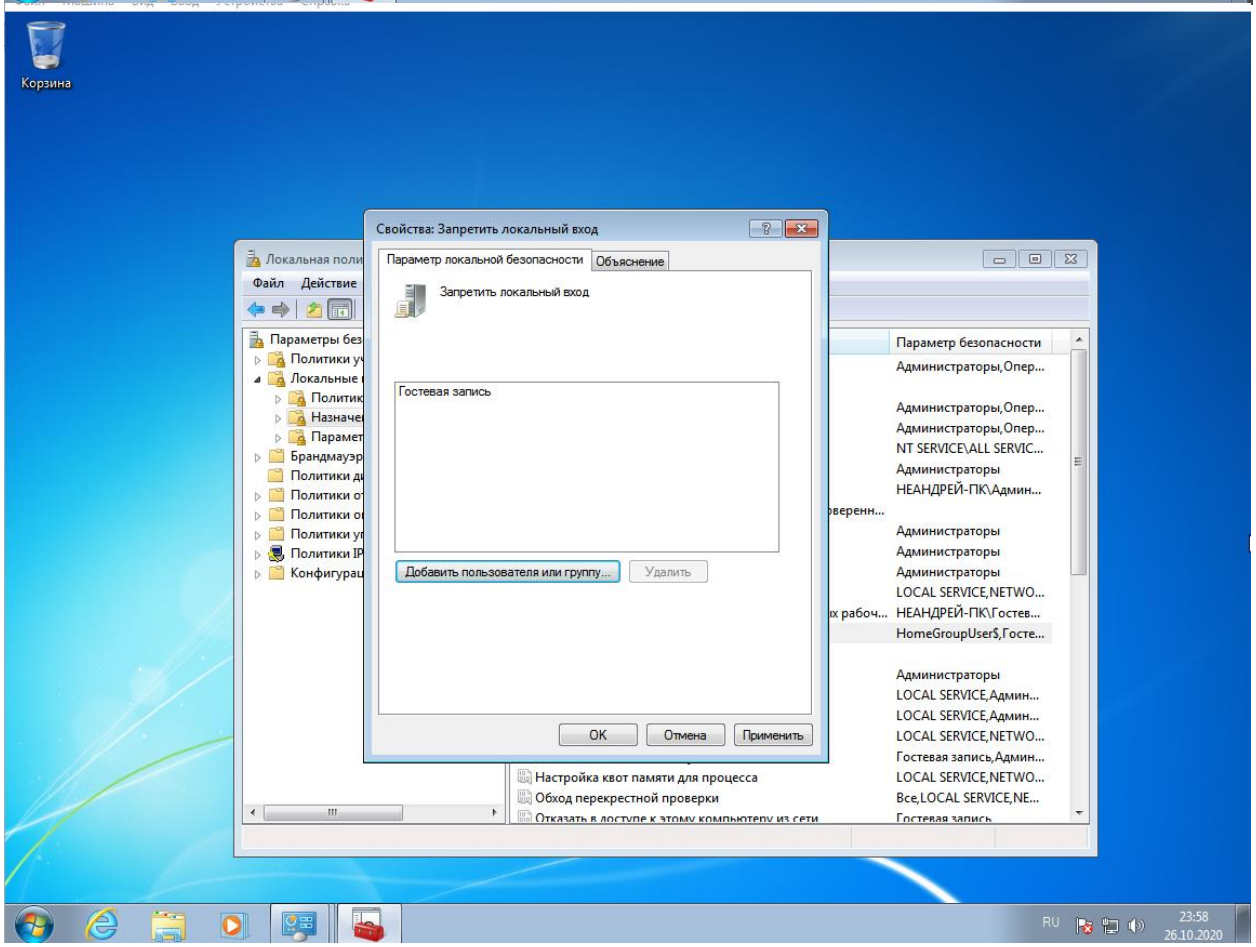

Корзина
Свойства: Запретить локальный вход
Параметр локальной безопасности
Объяснение
Запретить локальный вход
Гостевая запись
Добавить пользователя или группу...
Удалить
OK
Отмена
Применить
Параметр безопасности
Настройка квот памяти для процесса
Обход перекрестной проверки
RU
23:58
26.10.2020

Рисунок 13 - Изменение свойств «Запретить локальный вход» (Сверху - значение по умолчанию, снизу - пользовательская настройка)

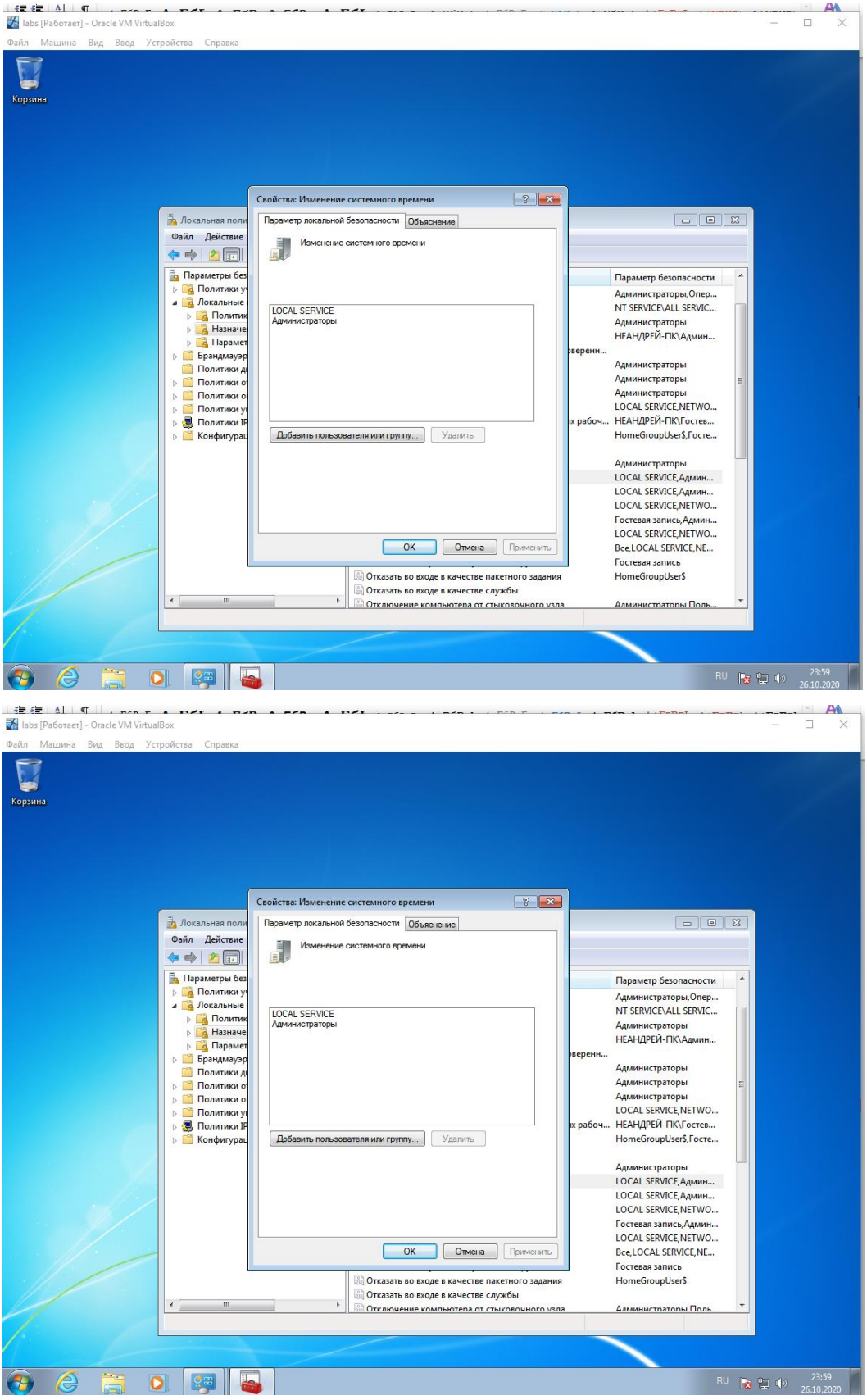


Рисунок 14 - Изменение свойств «Изменение системного времени» (Сверху - значение по умолчанию, снизу - пользовательская настройка)

3.7. *Журналы событий Windows*

В MicrosoftWindows *событие (event)* – это любое происшествие в операционной системе, которое записывается в журнал или требует уведомления пользователей или администраторов.

Для просмотра журналов Windows необходимо перейти по пути: Пуск → Поиск→ Просмотр журналов событий→ Просмотр событий → журналы Window

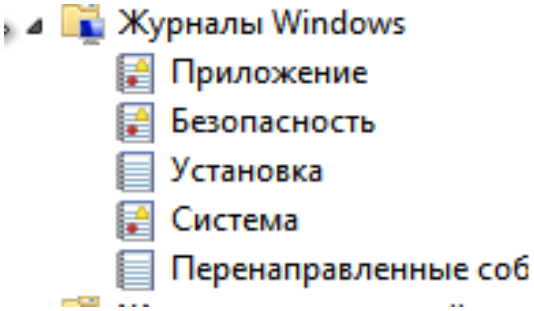


Рисунок 15 - Список журналов событий

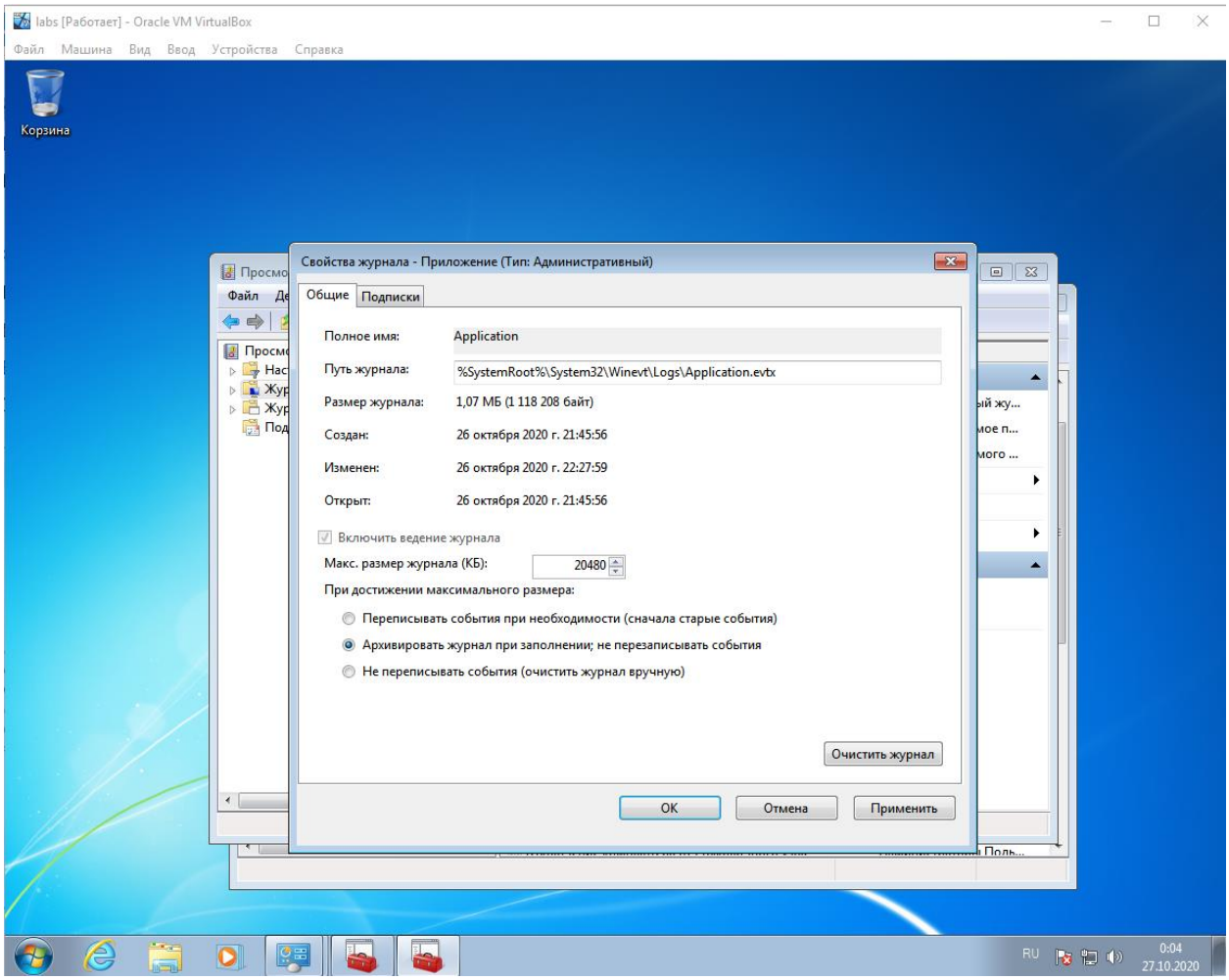


Рисунок 16 - Изменение свойств журнала

Выводы

Подсистема защиты от НСД – является важнейшим элементом в эшелонированной СЗИ на объектах информатизации. Правильная настройка подсистемы защиты от НСД

способно не только предотвратить угрозу, но и несет широкий спектр инструментов для анализа и совершенствования существующей СЗИ.

В результате лабораторной работы была произведена настройка локальных политик безопасности АРМ с установленной ОС Windows. Обоснование выбора и настройки параметров локальных политик безопасности базируются на требованиях к защите АРМ 17 от НСД как в «открытом», так и «закрытом» контуре. Настройка порядка хранения журналов Windows.