Цель работы:

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

Используемое программное обеспечение: операционная система Windows XP.

Основные сведения:

Локальная политика 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 автоматизированной системы предприятия. Для настройки локальной политики безопасности на автономном АРМ используется оснастка «Локальная политика безопасности». Если АРМ входит в состав домена, изменение политик, привязанных к домену Active Directory, можно настраивать при помощи оснастки «Редактор управления групповыми политиками».

Тип ИС закрытого контура в соответствие с вариантом – **2Б**

Требования к классу защищенности 2Б:

Подсистема управления доступом:

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.

Подсистема регистрации и учета:

Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная (при НСД);
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

Подсистема обеспечения целостности:

Должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;
- должны быть в наличии средства восстановления СЗИ НСД, предусматрива ющие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Подсистемы и требования	Класс 2Б
1. Подсистема управления доступом	
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	
в систему	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-
к программам	-
к томам, каталогам, файлам, записям, полям записей	-
1.2. Управление потоками информации	
2. Подсистема регистрации и учета	
2.1. Регистрация и учет:	
входа (выхода) субъектов доступа в (из) систему (узел сети)	+
выдачи печатных (графических) выходных документов	-
запуска (завершения) программ и процессов (заданий, задач)	-
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-
изменения полномочий субъектов доступа	-
создаваемых защищаемых объектов доступа	-

2.2. Учет носителей информации	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-
2.4. Сигнализация попыток нарушения защиты	-
3. Криптографическая подсистема	
3.1. Шифрование конфиденциальной информации	-
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-
4. Подсистема обеспечения целостности	
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+
4.3. Наличие администратора (службы) защиты информации в АС	-
4.4. Периодическое тестирование СЗИ НСД	+
4.5. Наличие средств восстановления СЗИ НСД	+
4.6. Использование сертифицированных средств защиты	-

Ход выполнения работы:

Согласно требованиям ИБ системы под пунктом 1.1 «Идентификация, проверка подлинности и контроль доступа субъектов», производим настройку политики ИБ.

Откроем «Политику паролей», перейдя по адресу:

Пуск → Выполнить → secpol.msc → Параметры безопасности → Политики учетных записей → Политика паролей

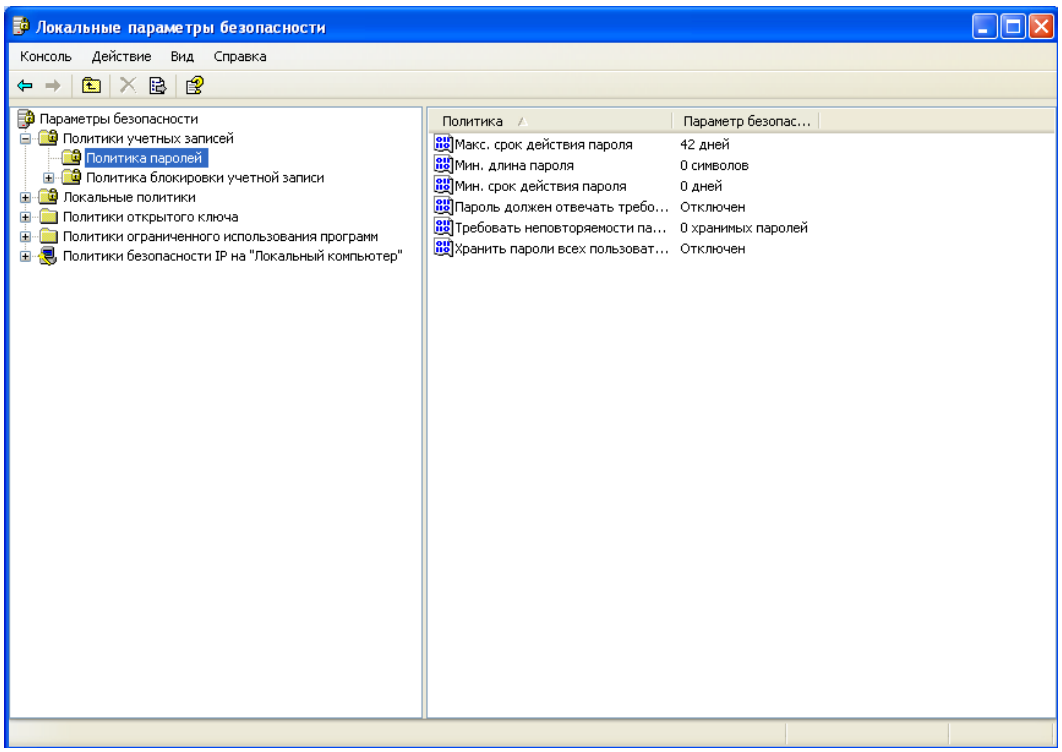

Рис.1 – Политика паролей по умолчанию

В результате настройки получили:

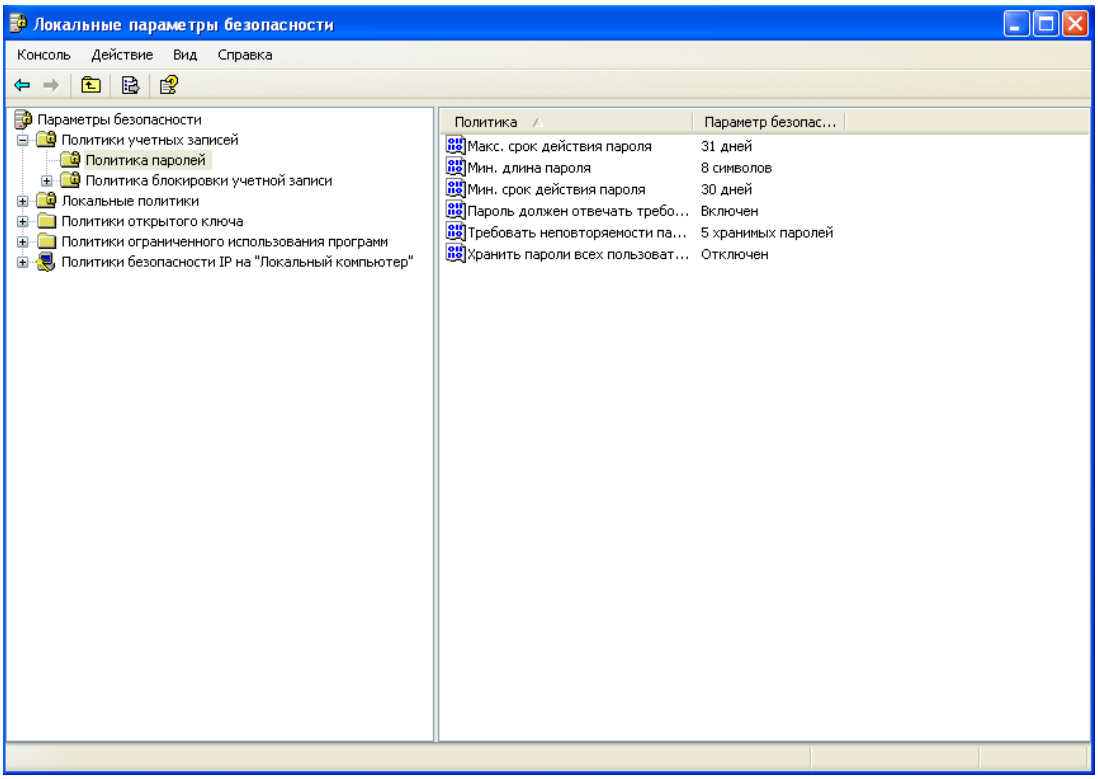

Рис.2 – Политика паролей после изменения

1) **Максимальны срок действия пароля** – выбрано значение в 31 день, то есть смена пароля должна проводиться раз в месяц

2) **Минимальный срок действия пароля** – выбрано значение в 30 дней, то есть пользователь сможет сменить пароль за день до окончания максимального срока.
3) **Минимальная длина пароля** – требования ФСТЭК требуют длину не менее 6 знаков, выбрано значение в 8 символов, как оптимальное. При желании можно увеличить длину пароля (либо уменьшить, но максимум до 6)
4) **Требования сложного пароля** – включено как необходимое требование безопасности, эта функция серьёзно повышает устойчивость пароля за счет значительного увеличения возможных вариантов.
5) **Требование неповторяемости паролей** – данная политика запрещает пользователю менять пароль на старый, установлено 5 неповторяемых паролей.
6) **Использование обратимого шифрования** – данная функция отключена, так серьёзно понижает устойчивость системы к атакам.

Согласно требованиям ИБ системы под пунктом 1.1 «Идентификация, проверка подлинности и контроль доступа субъектов», производим настройку политики ИБ.

Откроем «Политику блокировки учетной записи», перейдя по адресу:

Пуск → Выполнить → secpol.msc → Параметры безопасности → Политики учетных записей → Политика блокировки учетной записи

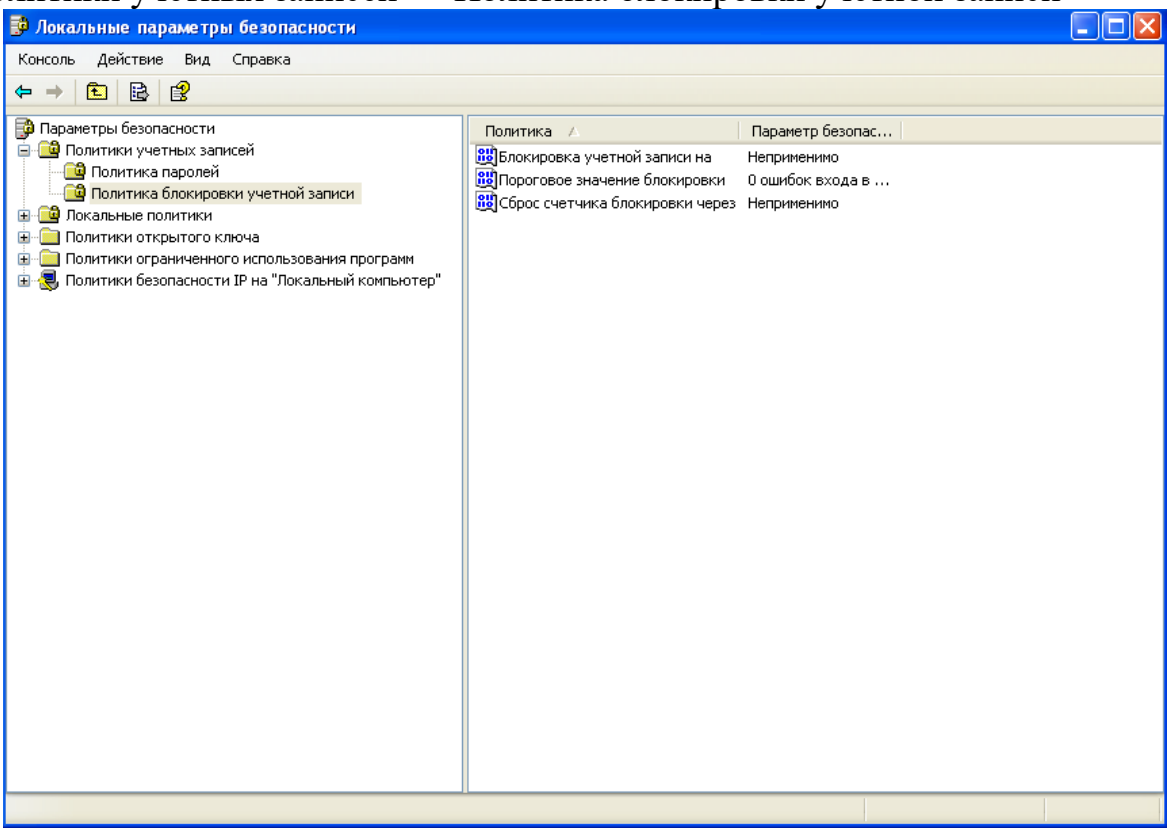

Рис.3 – Политика блокировки учетной записи по умолчанию

В результате настройки получили:

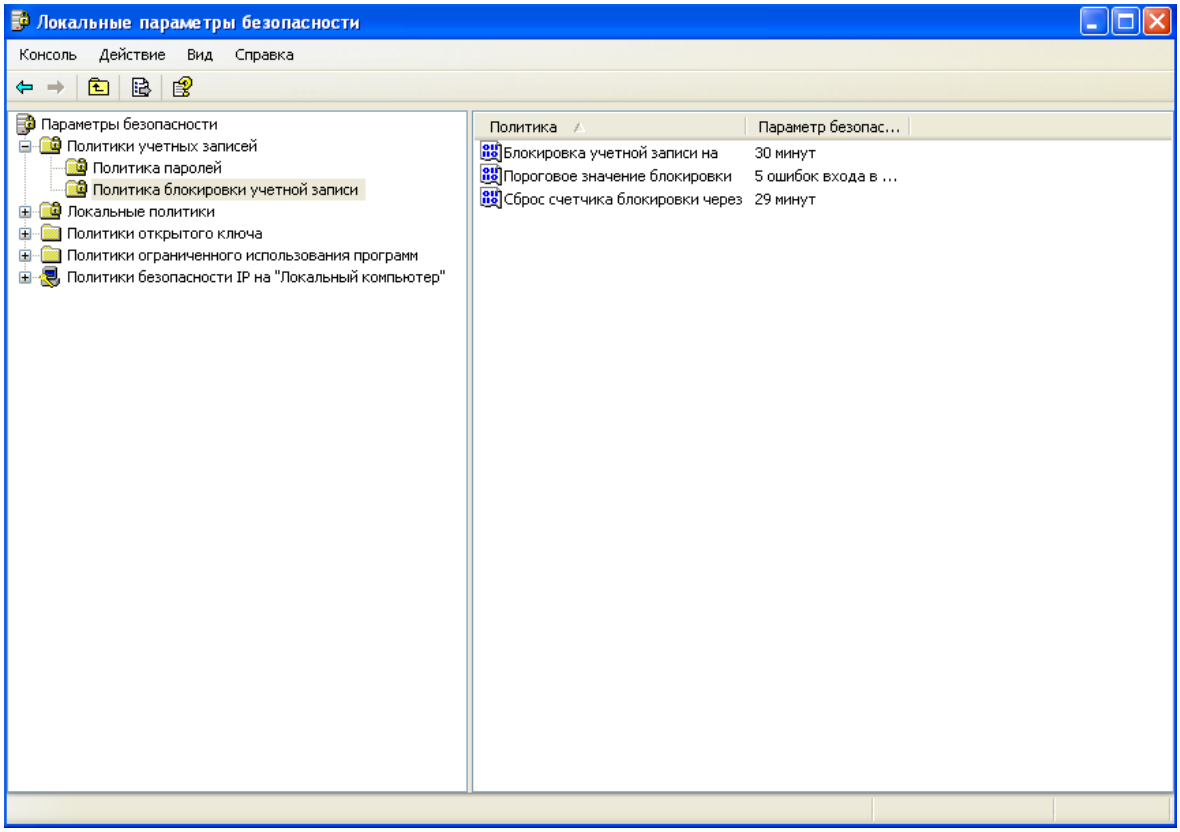

Рис.4 – Политика блокировки учетной записи после изменения

1) **Блокировка учетной записи** – определяет время блокировки входа, после исчерпания попыток входа. Установлено значение в 30 минут, поскольку это время останавливает работу сотрудника не на критичный промежуток времени, также этого времени достаточно на извещение службы безопасности о блокировке пользователя.
2) **Пороговое значение блокировки** – определяет количество попыток для входа в систему. Установлено значение в 5, что позволяет избежать блокировки пользователя из-за его невнимательности.
3) **Сброс счетчика блокировки** – установлено значение на минуту меньше времени блокировки, то есть счетчик сбрасывается перед самым концом блокировки пользователя.

Согласно требованиям ИБ системы под пунктом 1.1 «Идентификация, проверка подлинности и контроль доступа субъектов», 2.1 «Регистрация и учет», 4.1. «Обеспечение целостности программных средств и обрабатываемой информации», производим настройку политики ИБ.

Откроем «Политику блокировки учетной записи», перейдя по адресу:

Пуск → Выполнить → secpol.msc → Параметры безопасности → Локальные политики → Политика аудита

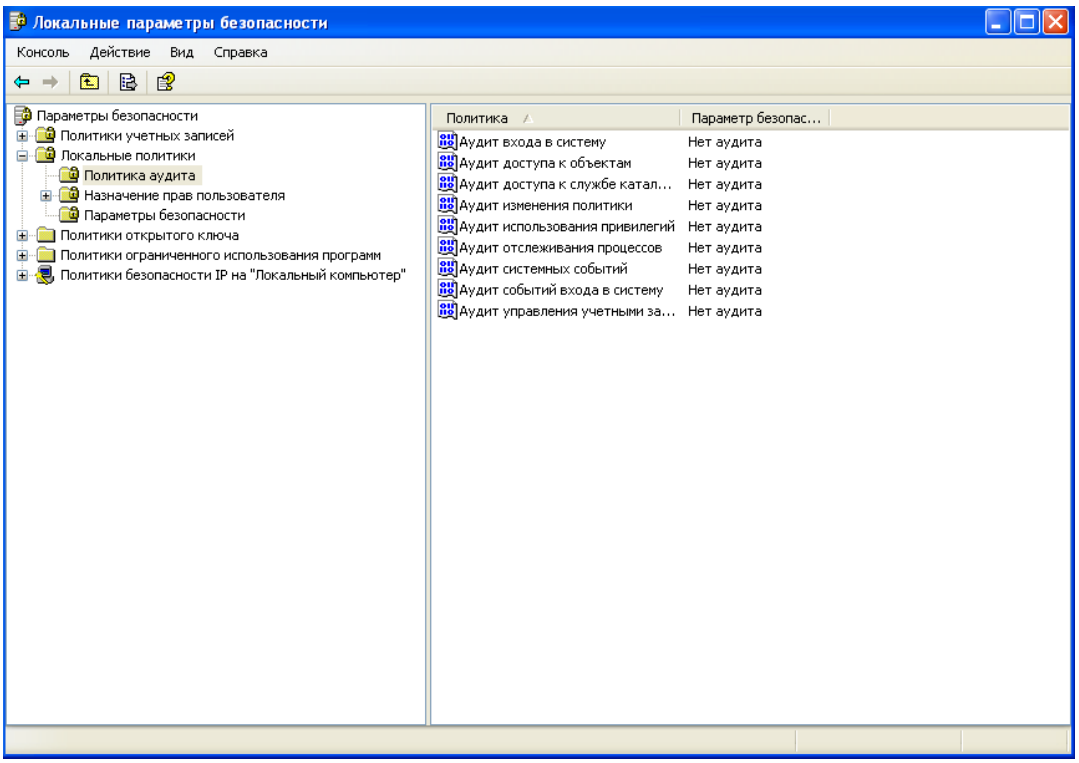

Рис.5 – Политики аудита по умолчанию

В результате настройки получили:

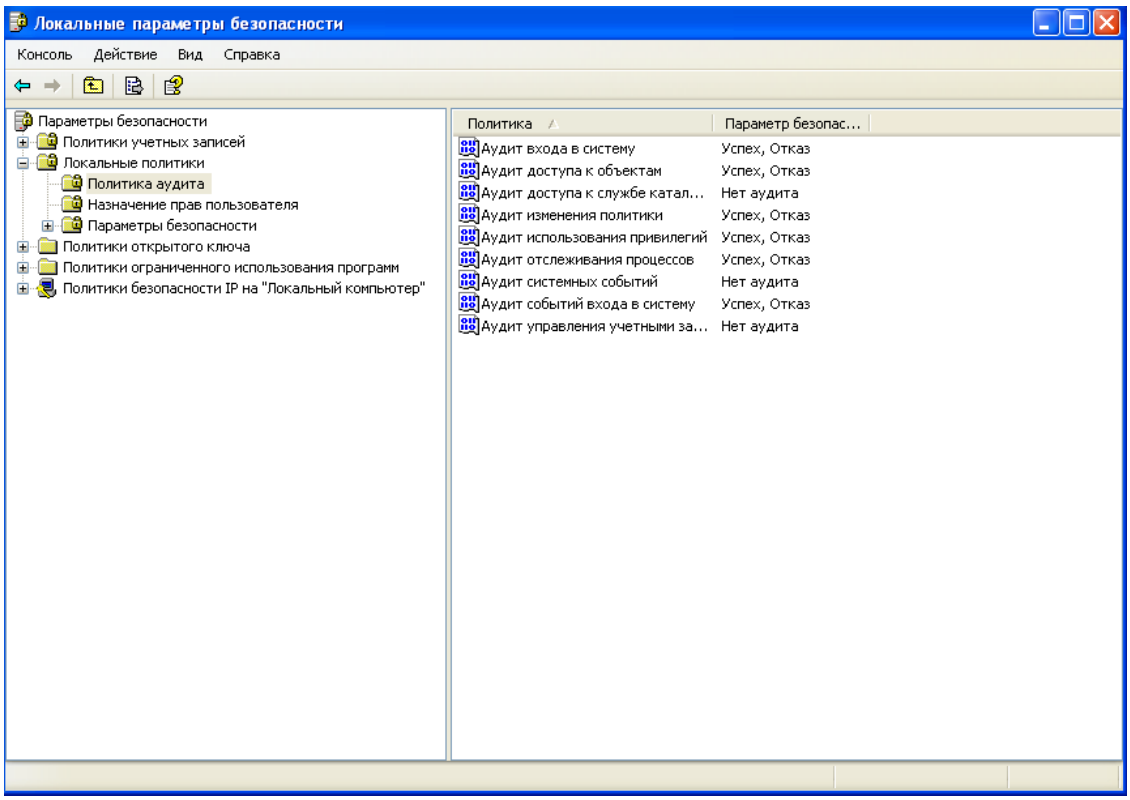

Рис.6 – Политики аудита после настройки

1) **Аудит входа в систему** – выполняет требование 1.1 «Идентификация, проверка подлинности и контроль доступа субъектов» и 2.1 «Регистрация и учет»

2) **Аудит доступа к объектам** – частично выполняет требование 4.1. «Обеспечение целостности программных средств и обрабатываемой информации»
3) **Аудит изменения политики** – не выполняет конкретных требований, но позволяет отслеживать опасные действия и проводить расследования
4) **Аудит использования привилегий** – не выполняет конкретных требований, но позволяет отслеживать опасные действия и проводить расследования
5) **Аудит отслеживания процессов** – частично выполняет требование 4.1. «Обеспечение целостности программных средств и обрабатываемой информации»
6) **Аудит событий входа в систему** - выполняет требование 1.1 «Идентификация, проверка подлинности и контроль доступа субъектов» и 2.1 «Регистрация и учет»

Выводы:

В результате выполнения ЛБ настроены политики ИБ АРМ с учетом требований ИБ к системе класса защищенности 2Б, а именно **1.1.** «Идентификация, проверка подлинности и контроль доступа субъектов», **2.1.** «Регистрация и учет», частично **4.1.** «Обеспечение целостности программных средств и обрабатываемой информации».

Это позволит частично выполнить требования ФСТЭК к классу защищенности 2Б.

Тем не менее встроенные политики не позволяют выполнить все требования к классу защищенности 2Б. Без защиты остались пункты 2.2. «Учет носителей информации», 4.2. «Физическая охрана средств вычислительной техники и носителей информации», 4.4. «Периодическое тестирование СЗИ НСД», 4.5. «Наличие средств восстановления СЗИ НСД» и частично 4.1. «Обеспечение целостности программных средств и обрабатываемой информации».

Таким образом, можно сделать вывод, что встроенные политики помогают специалисту по информационной безопасности, но не позволяют выполнить все требования к классу защищенности 2Б. Следовательно, нужно организовывать дополнительные мероприятия по защите информации и выделять средства на закупку специального программного обеспечения.