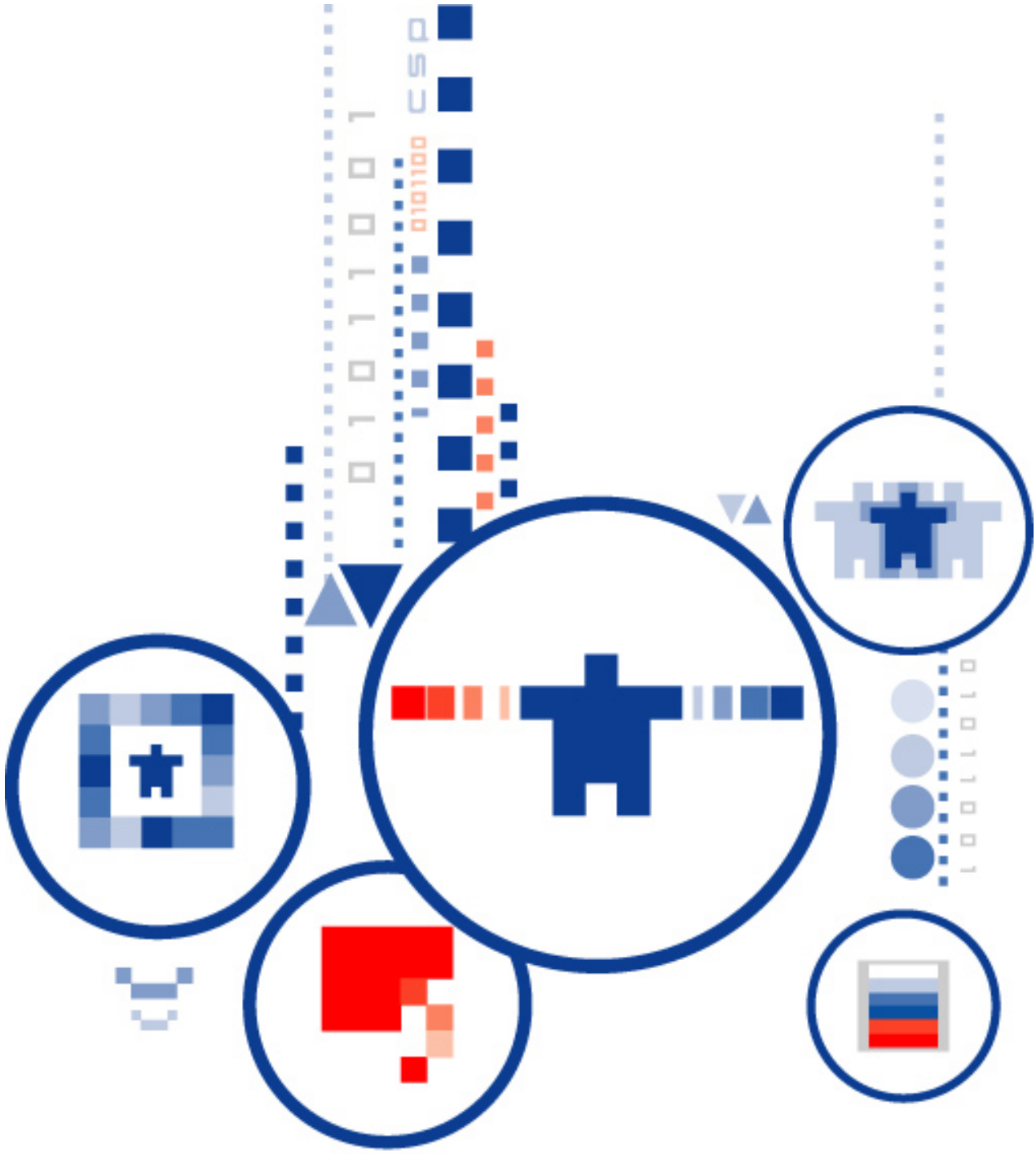
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 10-ЛУ

ЖТЯИ.00035-01 90 10



КриптоПро УЦ

программно-аппаратный комплекс
удостоверяющий центр

Руководство по безопасности

АННОТАЦИЯ

Настоящий документ содержит описание регламентных работ по обеспечению информационной безопасности при эксплуатации программного комплекса «Удостоверяющий Центр «КриптоПро УЦ» (УЦ).

Данное руководство предназначено для администратора безопасности УЦ или для администратора сетевых ресурсов предприятия, входящего в состав группы обслуживания УЦ.

Информация о разработчике ПК «КриптоПро УЦ»:

ООО "Крипто-Про"

127 018, Москва, улица Сущевский вал, 16 строение 5

Телефон: (495) 780 4820

Факс: (495) 780 4820

http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Введение 5
2. Настройка параметров TCP/IP MS Windows 2000 6
3. Использование СКЗИ КриптоПро CSP 7
4. Профиль защиты Удостоверяющего Центра 9
4.1. Перечень защищаемых объектов УЦ 9
4.2. Установки системы безопасности 9
4.2.1. Установки Windows Server 9
4.2.2. Установки Web-сервера MS IIS 10
4.2.3. Установки web-узла Центра Регистрации Web-сервера MS IIS 10
4.2.4. Установки виртуальных каталогов web-узла Центра Регистрации Web-сервера MS IIS 10
5. Использование и настройка межсетевых экранов 11
5.1. Использование межсетевых экранов 11
5.2. Настройка межсетевого экрана 11
6. Изолированный режим работы ПАК «КриптоПро УЦ» 13
7. Возможности нарушителя 14
8. Аудит Удостоверяющего Центра 15
8.1. Журналы событий Удостоверяющего Центра 15
8.1.1. Журнал событий Центра Сертификации 15
8.1.2. Журнал событий Центра Регистрации 15
8.1.3. Журнал событий АРМ администратора ЦР 15
8.2. Настройка аудита 15
8.2.1. Настройка аудита модуля политики службы сертификации ЦС 15
8.2.2. Настройка аудита в ПО Центра Регистрации 16
8.2.3. Настройка аудита в MS Windows 2000 16
8.2.4. Настройка аудита в MS Internet Information Server (IIS) 18
8.2.5. Настройка аудита в SQL 2000 Server 20
8.3. Структуры записей аудита 21
8.3.1. Структура записи аудита модуля политики службы сертификации ЦС 21
8.3.2. Структура записи аудита ПО Центра Регистрации 22
8.3.3. Структура записи аудита Windows 2000 Server 22
8.3.4. Структура записи аудита MS Internet Information Server (IIS) 23
8.3.5. Структура записи аудита SQL 2000 Server 24
8.4. Анализ журналов аудита 24
8.4.1. Анализ журнала модуля политики службы сертификации ЦС 24
8.4.2. Анализ журнала ПО Центра Регистрации 24
8.4.3. Анализ журналов в Windows 2000 Server 25
8.4.4. Анализ журналов в MS Internet Information Server (IIS) 27
8.4.5. Анализ журналов в SQL 2000 Server 29
8.5. Защита журналов аудита 30

8.5.1. Защита журнала модуля политики службы сертификации ЦС 30
8.5.2. Защита журнала ПО Центра Регистрации 30
8.5.3. Защита журналов событий MS Windows 2000 31
8.5.4. Защита журналов событий MS IIS 31
8.5.5. Защита журналов событий SQL 2000 Server 32
9. Смена паролей учетных записей ПК «КриптоПро УЦ» 33
10. Требования к серверным и рабочим помещениям удостоверяющего центра 36
10.1. Серверное помещение 36
10.2. Рабочие помещения 36
10.3. Архивохранилище 37

1. Введение

Угроза, реализованная с использованием уязвимостей информационно-программной системы, называется атакой.

Существует три основные категории атак:

- отказ в обслуживании;
- раскрытие информации;
- нарушение целостности.

Отказ в обслуживании (Denial of Service, DoS) – наиболее часто встречающийся на сегодняшний день вид нападения в Интернете, т.к. его можно выполнить удаленно и с высокой степенью анонимности.

Наиболее известные формы DoS-атак:

- захват всех ресурсов системы, в результате чего на долю авторизованных пользователей их не остается;
- аварийный останов системы – например, использование дефекта операционной системы (ОС), который приводит к нарушению прав доступа и в результате – к аварийному завершению работы ОС.

Раскрытие информации – следствие несанкционированного доступа к данным.

Нарушение целостности – умышленное искажение информации.

Наиболее подвержен сетевым атакам Центр Регистрации Удостоверяющего Центра, вследствие того, что он опубликован в локальной вычислительной сети.

Для обнаружения атак пользуются аудитом журналов (регистрационных файлов) общесистемного и прикладного программного обеспечения комплекса Удостоверяющего Центра. Такие журналы называются журналами аудита.

Целью аудита является сбор информации об удачных и неудачных попытках доступа к объектам, применении привилегий и других важных, с точки зрения безопасности, действиях и протоколирование этих событий для дальнейшего анализа.

2. Настройка параметров TCP/IP MS Windows 2000

С помощью программ REGEDIT установите параметры TCP/IP-стека в реестре Центра Сертификации и Центра Регистрации в соответствии с приведенными ниже значениями.

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=0

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableSecurityFilters=1

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=1

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=0

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery=0

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=300000

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=1

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions=2

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions=3

MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\NoNameReleaseOnDemand=1

Установка данных параметров увеличит сопротивляемость TCP/IP-стека распределенным атакам типа «отказ от обслуживания» (DDoS).

Подробнее об установке данных параметров см. на сайте http://www.microsoft.com/technet. Воспользуйтесь поиском по фразе “Security Considerations for Network Attacks”.

3. Использование СКЗИ КриптоПро CSP

Средство криптографической защиты (СКЗИ) КриптоПро CSP в Удостоверяющем Центре предназначено для:

- Использования в качестве средства ЭЦП при формировании, проверке электронной цифровой подписи (ЭЦП) и генерации ключей ЭЦП (ключей подписи и ключей обмена) в соответствии с отечественными стандартами ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34-11-94;
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
- контроля целостности программного обеспечения СКЗИ для его защиты от несанкционированного изменения или от нарушения правильности функционирования.
- управления ключами уполномоченного лица УЦ, сотрудников группы администрирования УЦ и пользователей УЦ.

Сертификат **СФ/114-1001** от "05" июня 2007 г., свидетельствует о том, что средство криптографической защиты информации (СКЗИ) "КриптоПро CSP (версия 2.0)" в составе согласно формуляру ЖТЯИ.00005-02 30 01 соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к СКЗИ класса КС1 (исполнение 3) или КС2 (исполнение 4) и может использоваться для формирования ключей шифрования и ключей электронной цифровой подписи, выработки и проверки электронной цифровой подписи, имитозащиты и шифрования информации, не содержащей сведений, составляющих государственную тайну. Сертификат подтверждает, что безопасность информации по уровню "КС2" обеспечивается при инсталляции и использовании СКЗИ в соответствии с требованиями нормативных документов формуляра ЖТЯИ.00005-02 30 01 и сохранении в тайне ключей шифрования и закрытых ключей электронной цифровой подписи.

Сертификат **СФ/124-0810** от "12" сентября 2005 г., свидетельствует о том, что средство криптографической защиты информации (СКЗИ) "КриптоПро CSP (версия 3.0)" в составе согласно формуляру ЖТЯИ.00015-01 30 01 соответствует требованиям ГОСТ 28147-89, ГОСТ Р34.10-94, ГОСТ Р34.10-2001 и требованиям к СКЗИ класса КС1 (КС2 при использовании совместно с сертифицированным средством защиты от НСД "Аккорд-АМДЗ" или "Соболь-РСО") и может использоваться для формирования ключей шифрования и ключей электронной цифровой подписи, выработки и проверки электронной цифровой подписи, имитозащиты и шифрования информации, не содержащей сведений, составляющих государственную тайну. Сертификат подтверждает, что безопасность информации по уровню "КС2" обеспечивается при инсталляции и использовании СКЗИ в соответствии с требованиями нормативных документов формуляра ЖТЯИ.00015-01 30 01 и сохранении в тайне ключей шифрования и ключей электронной цифровой подписи.

В процессе установки и эксплуатации ПО СКЗИ КриптоПро CSP в составе ПАК «КриптоПро УЦ» ЗАПРЕЩАЕТСЯ:

- добавлять считыватель информации из реестра («Реестр») в список установленных считывателей носителей секретных ключей;
- контейнеры закрытых ключей уполномоченного лица УЦ и сотрудников группы администрирования УЦ помечать как экспортируемые;
- копирование контейнеров закрытых ключей их владельцами;
- создавать контейнеры закрытых ключей без установленного пароля;
- использовать пароли:
    - длиной менее 6 символов;
    - мощность алфавита пароля менее 10 символов.

Указанные выше ограничения на использование СКЗИ КриптоПро CSP в составе ПАК «КриптоПро УЦ» должны быть включены в организационно-распорядительные и организационно-штатные документы Удостоверяющего Центра как организации в виде должностных инструкций и функциональных обязанностей.

4. Профиль защиты Удостоверяющего Центра

Положения профиля защиты информационных ресурсов Удостоверяющего Центра построены для предотвращения угроз со стороны пользователей, осуществляющих взаимодействие с Удостоверяющим Центром по сети.

Центр Регистрации Удостоверяющего Центра использует экземпляр SQL 2000 Server, работающий на локальном компьютере Центра Регистрации.

4.1. Перечень защищаемых объектов УЦ

Информационные ресурсы Удостоверяющего Центра, подлежащие защите, представляют собой совокупность следующих объектов Центра Регистрации:

- Web-сервер **MS IIS**;
- Web-узел Центра Регистрации сервера MS IIS (по умолчанию: **Веб-узел по умолчанию**);
- Виртуальный каталог **RA** web-узла Центра Регистрации и его содержимое;
- Виртуальный каталог **UI** web-узла Центра Регистрации и его содержимое;

Файлы содержимого виртуального каталога **RA** web-узла Центра Регистрации размещены в домашнем каталоге ..:\Documents and Settings\All Users\Application Data\Crypto Pro\RA\Inetpub\1\RA\ (значение ПО ЦР при установке по умолчанию).

Файлы содержимого виртуального каталога **UI** web-узла Центра Регистрации размещены в домашнем каталоге ..:\Documents and Settings\All Users\Application Data\Crypto Pro\RA\Inetpub\1\UI\ (значение ПО ЦР при установке по умолчанию).

4.2. Установки системы безопасности

4.2.1. Установки Windows Server

- для системного диска сервера Центра Регистрации должна быть определена файловая система NTFS;
- на домашние каталоги виртуальных каталогов web-узла Центра Регистрации должны быть установлены следующие разрешения:
  - Для администраторов: полный доступ
  - Для схемы СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ: полный доступ
  - Для группы «SYSTEM»: полный доступ
  - Для группы «ВСЕ»:
    - Чтение и выполнение;
    - Список содержимого папки;
    - Чтение.
- сервер Центра Регистрации не должен иметь сетевых дисков;
- ОС не должна содержать программных компонентов для обеспечения удаленного доступа к сети, маршрутизации протоколов и поддержки VPN (системные службы должны быть отключены);
- ОС не должна содержать средств удаленного администрирования;
- группа «Администраторы» должна содержать только учетные записи для реализации ролей **Системный администратор** (переименованная учетная запись **Администратор**) и **Администратор ЦР**;

- сервер Центра Регистрации не должен быть настроен как основной контроллер домена (PDC);
- ОС должна быть настроена для поддержки двух сетевых интерфейсов: один для взаимодействия с ЦС, другой для обеспечения сетевого взаимодействия пользователей с ЦР (внешний интерфейс);
- службы Windows Server не должны быть привязаны к внешнему интерфейсу, за исключением служб Web-сервера MS IIS;
- свойство **Auto Logon** не должно быть разрешено;
- учетная запись Guest должна быть отключена;
- В политике учетных записей параметров безопасности установить в качестве действующего параметра минимальную длину пароля 6 символов.

4.2.2. Установки Web-сервера MS IIS

- Web-сервер MS IIS должен быть установлен только со службой HTTP. Прочие службы не должны быть выбраны в качестве компонентов веб-сервера;
- удаленное администрирование IIS должно быть отключено;

4.2.3. Установки web-узла Центра Регистрации Web-сервера MS IIS

- идентификация веб-узла должна быть настроена на IP адрес внешнего интерфейса;
- должны быть удалены виртуальные каталоги MSADC, IISSamples, IISAdmin, IISHelp;
- должны быть установлены следующие веб-разрешения: чтение, запись в журнал и индексация каталога;
- должен быть разрешен только запуск сценариев.

4.2.4. Установки виртуальных каталогов web-узла Центра Регистрации Web-сервера MS IIS

- должны быть установлены следующие веб-разрешения: запись в журнал и индексация каталога;
- должен быть установлен уровень защиты: высокая (изолированная);
- в параметрах настройки приложения должны быть отключены флаги отладки;
- для виртуального каталога, предназначенного для публикации COC и доступа к его содержимому по протоколу HTTP (по умолчанию с именем CDP), должен быть запрещен запуск сценариев и исполняемых файлов.

5. Использование и настройка межсетевых экранов

5.1. Использование межсетевых экранов

Для защиты информационных ресурсов Удостоверяющего Центра при сетевом взаимодействии между компонентами УЦ и внешними приложениями (АРМ администратора и т.д.) с Центром Регистрации УЦ, необходимо использовать межсетевые экраны (брандмауэры).

Рекомендуемая схема соединения компонентов с использованием межсетевого экрана приведена на рисунке ниже.

Согласно приведенной выше схеме используется один межсетевой экран.

Должны использоваться межсетевые экраны не ниже 4-го класса в соответствии с «Временными требованиями к устройствам типа межсетевые экраны».

5.2. Настройка межсетевого экрана

1. Настройка пакетного фильтра на основе следующих правил фильтрации:
    a. Разрешить прохождение пакетов с IP адреса АРМ администратора ЦР на IP адрес ЦР
    b. Разрешить прохождение пакетов с IP адреса ЦР на IP адрес АРМ администратора ЦР и запретить прохождение пакетов с других IP адресов
    c. Разрешить прохождение пакетов с внешних IP адресов на IP адрес ЦР
    d. Разрешить HTTP как тип запрашиваемого сервиса и запретить другие типы запрашиваемых сервисов
    e. Разрешить порт 80 и 443 машины приемника и машины источника и запретить другие порты
2. Для правила фильтрации порта 80 IP адреса ЦР настроить механизм пассивных фильтров для анализа содержимого IP-пакетов на основе следующих правил:
    a. Запретить прохождение пакетов, поле данных которых содержит команды HTTP протокола (PUT, TRACE, DELETE, CONNECT) за исключением команды GET.

3. Настроить автоматическое протоколирование
4. Настроить удаленный мониторинг

6. Изолированный режим работы ПАК «КриптоПро УЦ»

Под изолированным режимом работы ПАК «КриптоПро УЦ» понимается комплекс организационно-технических мер, при выполнении которых нарушитель не располагает программно-аппаратными средствами взаимодействия с ПАК «КриптоПро УЦ».

Контролируемая зона – это пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц. В отношении контролируемой зоны действуют специальные правила, имеющие цель обеспечить защиту ПАК «КриптоПро УЦ» от несанкционированного доступа (по большому счету, обеспечить отсутствие каналов утечки информации).

Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения); ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения

Для обеспечения изолированного режима работы ПАК «КриптоПро УЦ» должны быть выполнены следующие меры:

- Компоненты ПАК «КриптоПро УЦ» должны располагаться в контролируемой зоне;
- Компоненты ПАК «КриптоПро УЦ» не должны иметь сетевых интерфейсов, подключенных к каналам связи, выходящим за пределы контролируемой зоны;
- Компоненты ПАК «КриптоПро УЦ» должны осуществлять взаимодействие по каналам связи, не выходящим за пределы контролируемой зоны;
- При установке программного обеспечения Центра Регистрации ПАК «КриптоПро УЦ» должен быть исключен из списка устанавливаемых компонентов **Веб-интерфейс пользователя**.

Дополнительно рекомендуется выполнить следующие меры:

- В составе технических средств Удостоверяющего Центра должно быть выделено рабочее место, не имеющее сетевых подключений к компонентам ПАК «КриптоПро УЦ» и программных закладок;
- Все внешние магнитные носители (типа дискет) должны перед использованием в компонентах ПАК «КриптоПро УЦ» проверяться на отсутствие программных закладок на рабочем месте, определенном в предыдущем пункте настоящих мер.

7. Возможности нарушителя

ПАК «КриптоПро УЦ» сертифицирован по уровню защиты КС2 с обеспечением информационной безопасности от воздействий нарушителей Н1 и Н2:

H_1 - внешний нарушитель, не являющийся пользователем, самостоятельно осуществляющий создание методов и средств реализации атак, а также самостоятельно реализующий атаки;

H_2 - внутренний нарушитель, не имеющий доступ к средствам вычислительной техники, на которых реализованы компоненты УЦ, за пределами контролируемой зоны являющийся пользователем, имеющим доступ к программно-аппаратным средствам взаимодействия с УЦ, самостоятельно осуществляющий создание методов и средств реализации атак, а также самостоятельно реализующий атаки;

При подключении ПАК «КриптоПро УЦ» к техническим средствам сетей общего пользования (внешних информационных систем) на ПАК «КриптоПро УЦ» может воздействовать потенциальный нарушитель с возможностями, превышающими возможности нарушителей Н1 и Н2.

8. Аудит Удостоверяющего Центра

8.1. Журналы событий Удостоверяющего Центра

8.1.1. Журнал событий Центра Сертификации

Журнал событий Центра Сертификации представляет собой совокупность журналов программных компонентов, работающих в составе Центра Сертификации:

- журнал событий модуля политики службы сертификации ЦС;
- журналы событий Windows Server 2000/2003 (журнал приложений, журнал безопасности и журнал системы);
- журнал событий MS Internet Information Server (MS IIS).

Настройка аудита событий, записываемых в журнал событий ЦС, выполняется в соответствии с разделом 8.2.

Анализ журнала событий ЦС выполняется в соответствии с разделом 8.3.

8.1.2. Журнал событий Центра Регистрации

Журнал событий Центра Регистрации представляет собой совокупность журналов программных компонентов, работающих в составе Центра Регистрации:

- журнал событий ПО ЦР;
- журналы событий Windows Server 2000/2003 (журнал приложений, журнал безопасности и журнал системы);
- журналы событий SQL Server 2000;
- журнал событий MS Internet Information Server (MS IIS).

Настройка аудита событий, записываемых в журнал событий ЦР, выполняется в соответствии с разделом 8.2.

Задачи переноса СОС на Центре Регистрации активно заполняют журнал событий «Приложение». Во избежание проблем с журналом, рекомендуется увеличить его размер из расчёта 45 Мб на одну задачу переноса

Анализ журнала событий ЦР выполняется в соответствии с разделом 8.3.

8.1.3. Журнал событий АРМ администратора ЦР

Журнал событий АРМ администратора Центра Регистрации выполнен в виде журналов событий Windows рабочего места администратора.

8.2. Настройка аудита

8.2.1. Настройка аудита модуля политики службы сертификации ЦС

Настройка аудита модуля политики службы сертификации ЦС не производится.

В журнале событий модуля политики автоматически регистрируются следующие события:

- запуск службы сертификации;
- останов службы сертификации;
- поступление запроса на сертификат;

- выпуск сертификата;
- отзыв сертификата;
- опубликование списка отозванных сертификатов.

8.2.2. Настройка аудита в ПО Центра Регистрации

Настройка аудита в ПО Центра Регистрации не производится.

В журнале событий ПО Центра Регистрации автоматически регистрируются следующие события:

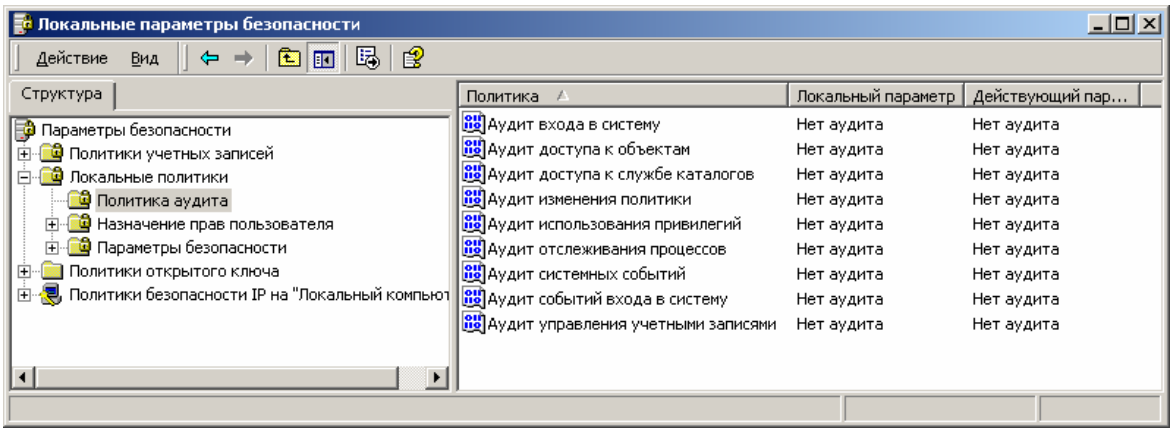
- Помещен запрос на регистрацию;
- Одобрен запрос на регистрацию;
- Отклонен запрос на регистрацию;
- Помещен запрос на сертификат;
- Одобрен запрос на сертификат;
- Отклонен запрос на сертификат;
- Установка сертификата подтверждена пользователем;
- Помещен запрос на отзыв сертификата;
- Одобрен запрос на отзыв сертификата;
- Отклонен запрос на отзыв сертификата;
- Помещен запрос на первый сертификат;
- Запрошен список отозванных сертификатов;
- Опубликован список отозванных сертификатов;
- Удален пользователь;
- Запрос на регистрацию не помещен в очередь;
- Запрос на регистрацию не одобрен;
- Запрос на регистрацию не отклонен;
- Запрос на сертификат не помещен;
- Запрос на сертификат не одобрен;
- Запрос на сертификат не отклонен;
- Установка сертификата не подтверждена;
- Запрос на отзыв сертификата не помещен;
- Запрос на отзыв сертификата не одобрен;
- Запрос на отзыв сертификата не отклонен;
- Запрос на первый сертификат не помещен;
- Список отозванных сертификатов не запрошен;
- Список отозванных сертификатов не опубликован;
- Пользователь не удален.

8.2.3. Настройка аудита в MS Windows 2000

В MS Windows 2000 можно настроить правила (политику) аудита на локальном компьютере, не входящем в домен. Если компьютер работает в домене, эти правила можно сделать глобальными.

Правила аудита настраиваются на всех компонентах Удостоверяющего центра, работающих под управлением MS Windows 2000 Server (Центр Сертификации, Центр Регистрации и на компьютере с SQL 2000 Server, в случае использования его в качестве выделенного сервера БД).

1. В утилите **Локальные параметры безопасности** (Security Policy) откройте узел **Локальные политики** (Local Policies), **Политика аудита** (Audit Policy).



2. Создайте политику в соответствии с приведенной ниже таблице:

Правило	**Параметры**
Audit account logon events (аудит регистрации учетных записей)	Success, Failure (удача, неудача)
Audit account management (аудит управления учетными записями)	Success, Failure (удача, неудача)
Audit directory services access (аудит доступа к службе каталогов)	Failure (неудача)
Audit logon events (аудит регистрации)	Success, Failure (удача, неудача)
Audit object access (аудит доступа к объектам)	Failure (неудача)
Audit policy change (аудит изменения политики)	Success, Failure (удача, неудача)
Audit privilege use (аудит использования привилегий)	Failure (неудача)
Audit process tracking (аудит отслеживания процессов)	No auditing (аудит отключен)
Audit system events (аудит системных событий)	No auditing (аудит отключен)

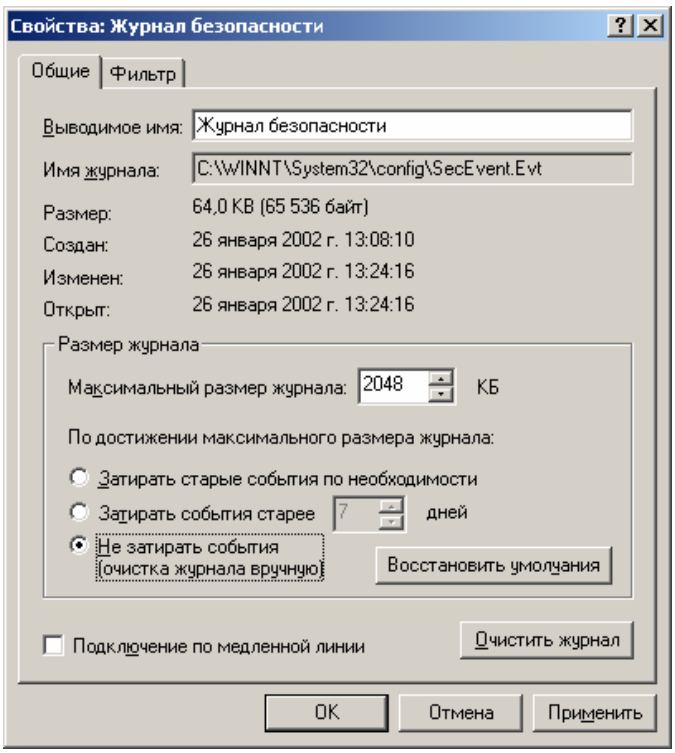
После определения параметров аудита необходимо настроить параметры журнала безопасности. Для этого выполните следующие действия:

Установка параметров журнала событий

1. Откройте окно «**Просмотр событий**» (Event Log) из группы программ «**Администрирование**».

2. В дереве консоли выберите **Журнал безопасности** (Security).

3. В меню **Действие (Action)** выберите команду **Свойства (Properties)**.



4. На вкладке **Общие (All)** установите требуемые параметры:

   4.1. Максимальный размер журнала – рекомендуется не менее 2Мб (2048 Кб)

   4.2. По достижении максимального размера журнала – не затирать события (очистка журнала вручную)

Для выполнения настройки аудита и параметров журнала безопасности необходимо войти в систему с учетной записью «Администратор» или члена группы «Администраторы».

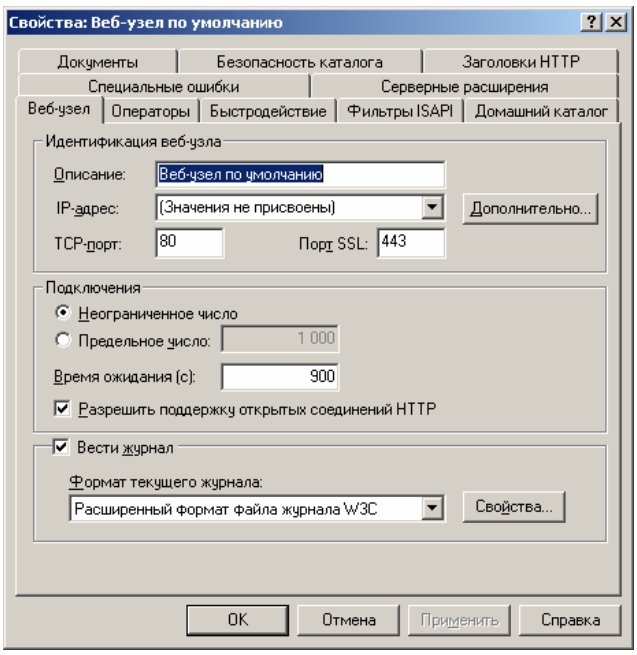
8.2.4. Настройка аудита в MS Internet Information Server (IIS)

Настройка аудита в MS IIS выполняется на Web-сервере Центра регистрации, т.к. он является (должен являться) единственным компонентом Удостоверяющего Центра, доступным в сети Интернет. Следовательно, он подвержен атакам хакеров.

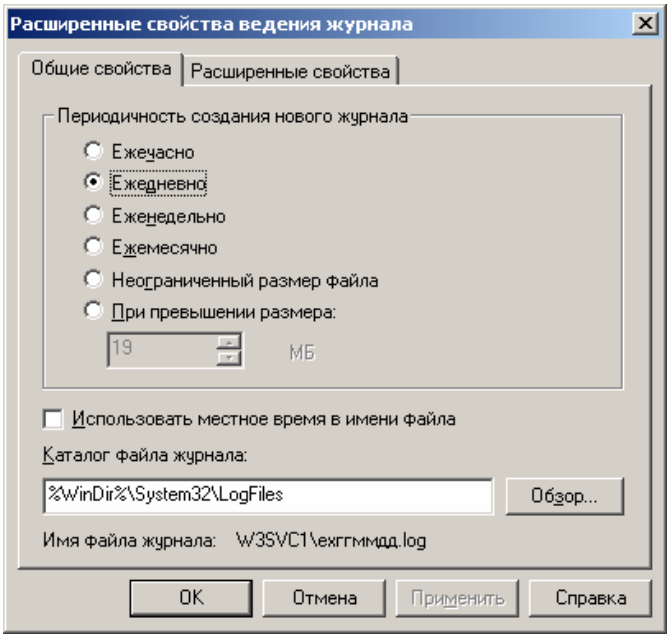
Для настройки аудита в MS IIS выполните следующие действия:

1. В модуле IIS Microsoft Management Console (MMC) щелкните правой кнопкой на Web-узле Центра Регистрации (по умолчанию, Default Web Site) и выберите в контекстном меню команду **Свойства** (Properties).

2. Проверьте, что установлен флажок Enable Logging, а в качестве формата журнала выбран W2C Extended Log File Format. Если флажок не установлен, то установите и выберите требуемый формат журнала.

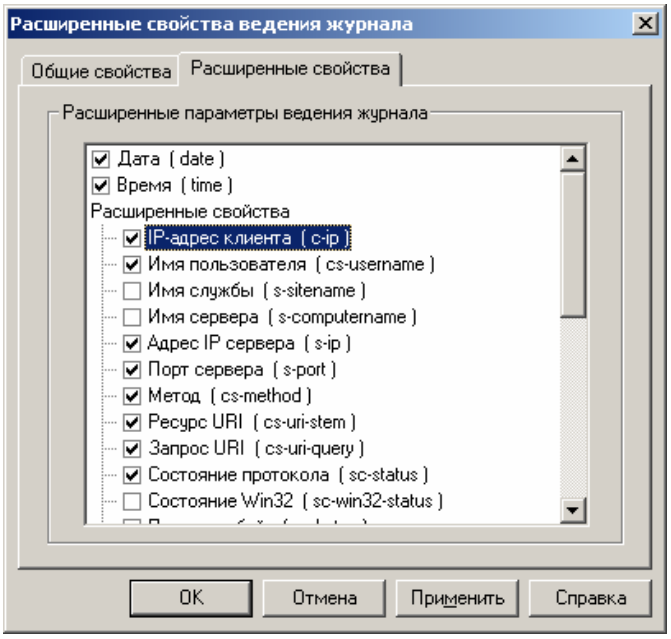


3. Щелкните кнопку **Свойства** (Properties) рядом с раскрывающимся списком **Формат текущего журнала** (Active Log Format).



4. Выберите новый временной период (периодичность создания нового журнала). Рекомендуемое значение – ежедневно. Если не хотите пользоваться принятым по умолчанию стандартом времени UTC (или GMT), включите параметр **Использовать местное время** (Use Local Time For Naming And Rollover).

5. Откройте вкладку **Расширенные свойства** (Extended Properties).

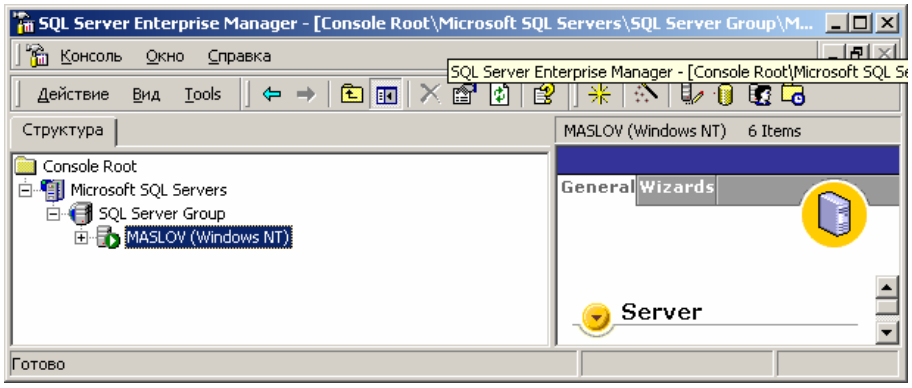


6. Убедитесь, что в отчет включены следующие элементы:
   a. Client IP Address (IP-адрес клиента);
   b. User Name (имя пользователя, получившего доступ к серверу);
   c. Method (метод, действие которое пытался выполнить клиент (например, POST));
   d. URI Stem (ресурс URI, т.е. ресурс к которому было выполнено обращение);
   e. URI Query (запрос URI, т.е. запрос который пытался выполнить клиент);
   f. Protocol Status (состояние протокола в терминах HTTP);
   g. Win32 Status (состояние Win32 в терминах Windows 2000);
   h. Bytes Sent (отправлено байт сервером);
   i. Bytes Received (получено байт сервером);
   j. Time Token (время, которое заняло действие);
   k. User Agent (агент пользователя, т.е. обозреватель пользователя).

8.2.5. Настройка аудита в SQL 2000 Server

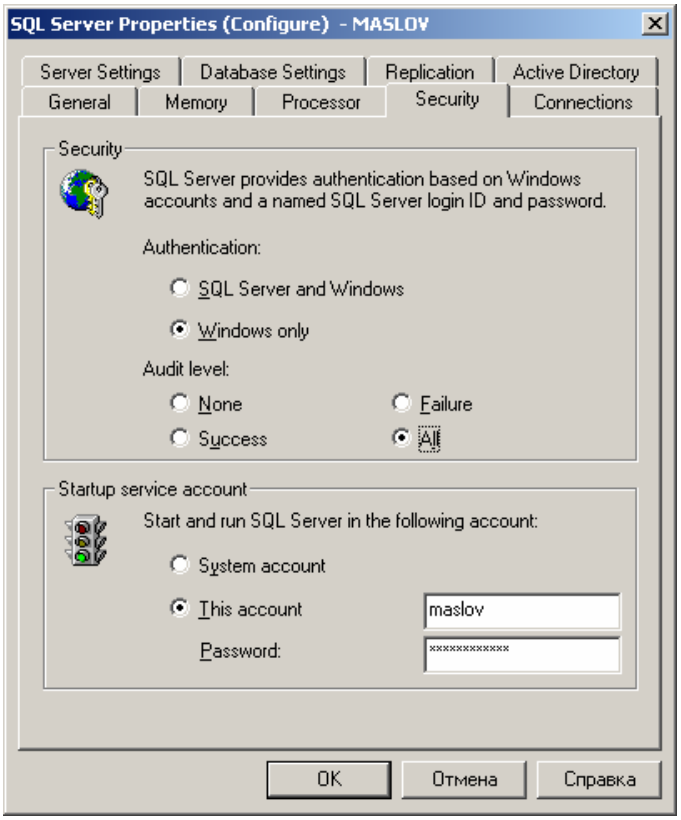
Для настройки аудита в SQL 2000 Server Центра Регистрации выполните следующие действия:

1. В SQL Server Enterprise Manager раскройте узлы Microsoft SQL Servers, SQL Server Groups.
2. Раскройте узел SQL Server Центра Регистрации.



3. Щелкните сервер правой кнопкой и выберите в контекстном меню команду **Properties**.

4. Откройте вкладку **Security**.



5. Убедитесь, что в списке Audit Level выбрано значение All, и щелкните кнопку OK.

8.3. Структуры записей аудита

8.3.1. Структура записи аудита модуля политики службы сертификации ЦС

Поле	Описание
Время	Дата и время (разделенные пробелом), когда произошло данное событие
Событие	Код типа данного события
ID запроса	Идентификатор запроса на сертификат
Subject запроса	Группа значений, разделенная запятыми, определяющая субъекта запроса
Usage запроса	Группа значений, разделенная запятыми, определяющая области использования запрашиваемого сертификата в запросе

Subject сертификата	Группа значений, разделенная запятыми, определяющая субъекта (владельца) сертификата открытого ключа
Usage сертификата	Группа значений, разделенная запятыми, определяющая области использования сертификата открытого ключа
Serial сертификата	Серийный (регистрационный) номер сертификата
FileName COC	Имя файла, содержащий сформированный список отозванных сертификатов (CRL)

Дополнительная информация при детализации события, располагается после поля **Событие**, зависит от типа события и содержит группу полей. Поля, не заполняемые при детализации события, заполняются пустым значением.

Все поля в записи журнала аудита разделяются знаком табуляции.

8.3.2. Структура записи аудита ПО Центра Регистрации

Поле	Описание
EventID	Уникальный идентификатор данного события
EventTypeID	Идентификатор типа данного события, определенного в таблице EventType
EventDate	Дата, когда произошло данное событие
EventDescripton	Текстовое описание данного события
UserID	Идентификатор пользователя, который выполнил задачу, породившую данное событие и определенного в таблице UserInfo1
SubjectID	Идентификатор пользователя, являющийся субъектом для которого выполнялась задача, породившая данное событие, и определенного в таблице UserInfo1

8.3.3. Структура записи аудита Windows 2000 Server

Поле	Описание
Дата	Дата, когда произошло данное событие.
Время	Локальное время, когда произошло данное событие.
Пользователь	Имя пользователя, действия которого привели к данному событию. Это имя соответствует коду процесса клиента, если событие было вызвано процессом-сервером, и коду основного процесса в случае, если пользователь не причастен к событию. В некоторых случаях запись журнала безопасности содержит оба кода. (Олицетворение происходит в тех случаях, когда в Windows 2000 один процесс присваивает атрибуты безопасности другого процесса.)
Компьютер	Имя компьютера, на котором произошло событие. Обычно это имя локального компьютера, если только просмотр событий не выполняется с другого компьютера Windows 2000.
Код события	Число, определяющее конкретный тип события. В первой строке описания обычно содержится название типа события. Например, 6005 — это идентификатор события, которое происходит при запуске службы ведения журналов событий. Соответственно, в начале описания этого события находится строка «Запущена служба журнала событий». Код события и имя источника записи могут использоваться представителями группы поддержки программного продукта для устранения неполадок.
Источник	Программа, занесшая событие. Это может быть как имя программы (например, «SQL Server»), так и название компонента системы или большого приложения (например, название драйвера). Например, «Elnkii» означает драйвер EtherLink II.

Тип	Уровень важности события: «Ошибка», «Уведомление» или «Предупреждение» в журналах системы и приложений; «Аудит успехов» или «Аудит отказов» в журнале безопасности. В окне просмотра событий тип события представлен соответствующим значком.
Категория	Категория события в зависимости от источника события. Это сведения используются преимущественно в журнале безопасности. Например, для аудита событий безопасности категория соответствует одному из типов событий, для которых в групповой политике может быть включен аудит успехов или отказов.

8.3.4. Структура записи аудита MS Internet Information Server (IIS)

Поле	Обозначение в журнале аудита	Описание
Дата	`date`	Дата возникновения события.
Время	`time`	Время возникновения события.
IP-адрес клиента	`c-ip`	IP-адрес клиента, получившего доступ к серверу.
Имя пользователя	`c-username`	Имя пользователя, получившего доступ к серверу. Это не относится к анонимным пользователям, которые обозначаются черточками.
Имя службы	`s-sitename`	Служба Интернета, выполнявшаяся на компьютере клиента, и номер экземпляра.
Имя сервера	`s-computername`	Имя сервера, на котором была создана запись журнала.
Адрес IP сервера	`s-ip`	IP-адрес сервера, на котором была создана запись журнала.
Метод	`cs-method`	Действие, которое пытался выполнить клиент (например, метод GET).
Ресурс URI	`cs-uri-stem`	Ресурс, к которому было выполнено обращение, например Default.htm.
Запрос URI	`cs-uri-query`	Запрос, который пытался выполнить клиент.
Состояние протокола	`sc-status`	Состояние действия (в терминах HTTP).
Состояние Win32	`sc-win32-status`	Состояние действия (в терминах Windows 2000).
Передано байт	`sc-bytes`	Число байт, отправленных сервером.
Получено байт	`cs-bytes`	Число байт, полученных сервером.
Порт сервера	`s-port`	Номер порта, к которому подключен клиент.
Заняло времени	`time-taken`	Время, которое заняло выполнение действия.
Версия протокола	`cs-protocol`	Версия протокола (HTTP, FTP), используемого клиентом. Для протокола HTTP это либо HTTP 1.0, либо HTTP 1.1.
Агент пользователя	`cs(User-Agent)`	Обозреватель, используемый клиентом.
Объект Cookie	`cs(Cookie)`	Содержимое отправленного или полученного модуля настройки клиента (cookie) (если имеется).

Источник ссылки	cs(Referer)	Предыдущий просмотренный пользователем узел. На этом узле содержалась ссылка на данный узел.

Все поля в записи журнала аудита разделяются пробелами.

8.3.5. Структура записи аудита SQL 2000 Server

Поле	Описание
Дата	Дата возникновения события.
Время	Время возникновения события.
Процесс	Имя серверного процесса
Описание	Текстовое описание события

Все поля в записи журнала аудита разделяются пробелами.

8.4. Анализ журналов аудита

8.4.1. Анализ журнала модуля политики службы сертификации ЦС

Файл журнала аудита модуля политики службы сертификации ЦС располагается в каталоге %WinDir%\Program Files\Crypto Pro\CA\log (по умолчанию) и имеет наименование CA.log по умолчанию.

Формат записи в файле в кодах ASCII с полями, разделенными символом табуляции.

Анализ журнала, созданного модулем политики службы сертификации ЦС, может быть выполнен путем просмотра в текстовых редакторах, но рекомендуется использовать программы-генераторы отчетов.

Таблица 1. Таблица кодов событий службы сертификации ЦС

Код события	Описание события
1	Сертификат издан
2	Сертификат переведен в ожидание
4	Выпуск сертификата отклонен
8	Сертификат отозван (приостановлен, возобновлен)
16	Из БД службы сертификации получен ранее переведенный в ожидание сертификат
32	Издан новый список отозванных сертификатов
64	Служба сертификации остановлена (сообщение модуля выхода)
128	Служба сертификации запущена (сообщение модуля выхода)
100	Запущен модуль политики
101	Модуль политики остановлен
102	Модуль политики закончил обработку запроса на сертификат с кодом успеха VR_INSTANT_OK
200	Файл со списком отозванных сертификатов успешно записан в каталог CDP

8.4.2. Анализ журнала ПО Центра Регистрации

Журнал аудита ПО Центра Регистрации представляет собой совокупность таблиц EventLog и EventType в базе данных Центра Регистрации.

Анализ журнала аудита может выполняться двумя способами:

- с использованием средств, предоставляемых ПО АРМ администратора ЦР;
- с использованием программ-генераторов отчетов.

8.4.3. Анализ журналов в Windows 2000 Server

В Windows 2000 Server ведутся три журнала событий: журнал приложений, журнал безопасности и журнал системы.

Журнал приложений – содержит ошибки, предупреждения или информацию программ. Записываемые события определяются разработчиками программ.

Журнал системы – содержит ошибки, предупреждения и дополнительную информацию, генерируемые Windows 2000. Перечень наблюдаемых событий задает Windows 2000.

Журнал безопасности содержит сведения об успешных и безуспешных попытках доступа в систему, а также о событиях, относящихся к использованию ресурсов, таких как создание, открытие и удаление файлов и других объектов. Например, если разрешен аудит входа в систему, все попытки входа в систему будут заноситься в журнал безопасности.

Журналы приложений и системы доступны для просмотра и обработки всем пользователям. Журнал безопасности доступен для анализа только пользователю, вошедшему в систему с учетной записью «Администратор» или входящему в группу «Администраторы».

В журнал безопасности заносятся события двух типов:

- аудит успехов;
- аудит отказов.

Событие «аудит успеха» - это событие, соответствующее успешно завершенному действию, связанному с поддержкой безопасности системы. Например, в случае успешного входа пользователя в систему в журнал заносится событие типа «Аудит успехов».

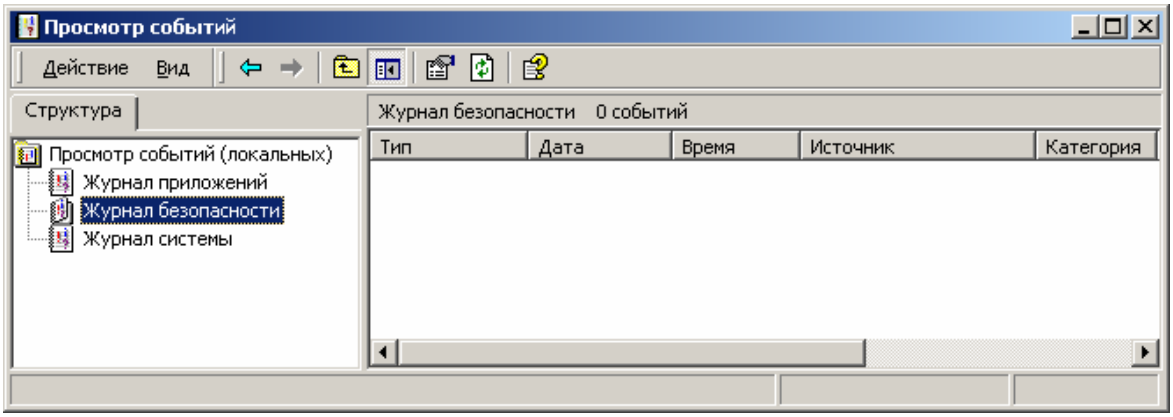
Событие «аудит отказа» - это событие, соответствующее неудачно завершенному действию, связанному с поддержкой безопасности системы. Например, в случае неудачной попытки доступа пользователя к сетевому диску в журнал заносится событие типа «Аудит отказов».

Заголовок события безопасности содержит следующие сведения.

Сведения	**Значение**
Дата	Дата, когда произошло данное событие.
Время	Локальное время, когда произошло данное событие.
Пользователь	Имя пользователя, действия которого привели к данному событию. Это имя соответствует коду процесса клиента, если событие было вызвано процессом-сервером, и коду основного процесса в случае, если пользователь не причастен к событию. В некоторых случаях запись журнала безопасности содержит оба кода. (Олицетворение происходит в тех случаях, когда в MS Windows 2000 один процесс присваивает атрибуты безопасности другого процесса.)
Компьютер	Имя компьютера, на котором произошло событие. Обычно это имя локального компьютера, если только просмотр событий не выполняется с другого компьютера MS Windows 2000.
Код события	Число, определяющее конкретный тип события. В первой строке описания обычно содержится название типа события. Например, 612 — это идентификатор события, которое происходит при изменении правил аудита.

Источник	Программа, занесшая событие. Это может быть как имя программы (например, «SQL Server»), так и название компонента системы или большого приложения (например, название драйвера). Например, «Elnkii» означает драйвер EtherLink II.
Тип	Тип события: «Аудит успехов» или «Аудит отказов». В окне просмотра событий тип события представлен соответствующим значком.
Категория	Категория соответствует одному из типов событий, для которых в групповой политике может быть включен аудит успехов или отказов.

Анализ журнала безопасности производится с использованием средства просмотра событий (Event Viewer). Данное средство входит в состав средств администрирования локального компьютера и доступно через **Пуск** ->**Программы**->**Администрирование**->**Просмотр событий**.



При анализе журнала безопасности следует обращать особое внимание на следующие события:

Код события	Комментарий
612	Изменены правила аудита
640	Изменена база данных SAM
531	Попытка регистрации по отключенной записи
539	Попытка регистрации, отклоненная из-за того, что учетная запись заблокирована
529	Попытка регистрации с помощью неизвестной учетной записи пользователя или с помощью допустимой учетной записи, но неправильным паролем (неожиданное увеличение числа таких событий может указать на попытки подобрать пароль)
517	Был очищен журнал аудита
624	Была создана учетная запись пользователя
628	Был установлен пароль учетной записи пользователя

Анализ журнала безопасности рекомендуется производить не реже одного раза в сутки.

Для предотвращения переполнения журнала безопасности необходимо регулярно производить процедуру очистки журнала безопасности.

Очистка журнала безопасности выполняется следующим образом:

1. Откройте окно «**Просмотр событий**» (Event Viewer).
2. В дереве консоли выберите журнал, который нужно очистить.
3. В меню **Действие (Action)** выберите команду **Стереть все события**.
4. Чтобы сохранить журнал перед очисткой, нажмите кнопку **Да**.
5. Нажмите кнопку **Нет** для уничтожения текущих записей журнала и начала регистрации новых событий.

При переполнении журнала безопасности операционная система Windows 2000 перестает отвечать на запросы и выводит сообщение «Неудачная попытка аудита». В этом случае выполните следующие действия:

1. Перезагрузите компьютер и войдите в систему с учетной записью из группы администраторов.
2. Откройте окно **Просмотр событий (Event Viewer)**.
3. Сохраните события текущего журнала в файл.
4. Очистите все события из журнала безопасности.
5. Откройте редактор реестра и найдите следующий раздел:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
6. Удалите и замените значение параметра CrashOnAuditFail типом данных REG_DWORD и значением 1.
7. Закройте редактор реестра и перезагрузите компьютер.

8.4.4. Анализ журналов в MS Internet Information Server (IIS)

Файлы журнала аудита MS IIS располагаются в каталоге %WinDir%\System32\LogFiles (по умолчанию) и имеют наименование в шаблоне ГГГГММДД.log, где ГГГГ - четырехзначный год, ММ – месяц, ДД - день.

Формат записи в файле в кодах ASCII с полями, разделенными пробелами.

Журналы, созданные MS IIS, могут быть прочитаны в текстовых редакторах, но рекомендуется использовать программы-генераторы отчетов.

Для анализа журналов на предмет обнаружения возможных атак с использованием сценариев, написанных для уже известных и устраненных проблем, воспользуйтесь сведениями о наиболее распространенных атаках на IIS, приведенных в таблице ниже.

Атака	Комментарий
Ошибка «::$DATA»	Позволяет атакующему просмотреть исходный код ASP-файлов приложения
Ошибка «.»	Аналогична предыдущей
Переполнение буфера «.htr»	Специально подготовленный запрос к .htr-файлу исполняет произвольный код в контексте защиты Web-сервера
Применение RDS	Специально подготовленный запрос Remote Data Services исполняет произвольный код на сервере

Признаком того, что Web-сервер Центра Регистрации подвергается или подвергся атаке (с большой долей вероятности), является наличие в журнале IIS следующих записей:

Атака	Пример(ы) записей журнала
Ошибка «::$DATA»	15:59:09 218.216.157.240 – W3SVC1 207.46.171.196 80 GET / default.asp::$DATA
Ошибка «.»	15:59:09 218.216.157.240 – W3SVC1 207.46.171.196 80 GET / default.asp. (обратите внимание на «.» в конце строки)
Переполнение буфера «.htr»	15:59:09 218.216.157.240 – W3SVC1 207.46.171.196 80 GET / iisadmwd/aexp.htr
Применение RDS	15:59:09 218.216.157.240 – W3SVC1 207.46.171.196 80 POST /msadc/msadcs.dll hr=800a1004,CsoapStub::HttpExtensionProc, 200 271 679
	15:59:09 218.216.157.240 – W3SVC1 207.46.171.196 80 GET /msadc/msadcs.dll – 404 3395 387
	15:59:09 218.216.157.240 – W3SVC1 207.46.171.196 80 GET /msadc/msadcs.dll/VbBusObj.VbBusObjCls.GetRecordset+HTTP/1.1 – 404 3395 387
	15:59:09 218.216.157.240 – W3SVC1 207.46.171.196 80 GET /msadc/msadcs.dll/AdvancedDataFactory.Query+HTTP/1.1 – 401 3417 452

Поиск таких записей в журнале может выполняться программным способом.

Текст одной из программ на языке Perl по обработке записей в журналах аудита MS IIS приведен ниже:

```
#!/usr/bin/perl
$SUMMARY_ONLY = 0;       # Set to 0 to display offending all lines
%hits=(RDS               => 0,
        DOLLAR_DATA      => 0,
        DOT              => 0,
        SAMPLES          => 0,
        SHOWCODE         => 0,
        HTR              => 0,
        DOT_DOT          => 0,
        SAM_ACCESS       => 0,
        INDEX            => 0,
        BOOT_INI         => 0);
foreach (<$ARGV[0]>) {
        printf "Opening log $_(%s)", (-e $_) ? "Cool!" : "Not Cool!";
        warn unless open FILEHANDLE, "<" . $_;
        # read each line
        while (<FILEHANDLE>) {
                print "$lines lines processed.\r" if ++$lines % 500 == 0;
                if (/msadcs/i) {
                        print "[RDS EXPLOIT] $_\n" unless $SUMMARY_ONLY;
                        $hits{RDS}++;
                } elsif (/::\$DATA/i) {
                        print "[::\$DATA EXPLOIT] $_\n" unless $SUMMARY_ONLY;
                        $hits{DOLLAR_DATA}++;
                } elsif (/.*GET \/.*\.asp\./i) {
                        print "['.' EXPLOIT] $_\n" unless $SUMMARY_ONLY;
                        $hits{DOT}++;
                } elsif (/sam\._/i) {
                        print "[ACCESSING SAM] $_\n" unless $SUMMARY_ONLY;
```

```
                        $hits{SAM_ACCESS}++;
                } elsif (/\.ida|\.idq|\.htw/i) {
                        print "[INDEX SERVER] $_\n" unless $SUMMARY_ONLY;
                        $hits{INDEX}++;
                } elsif (/boot\.ini/i) {
                        print "[ACCESSING BOOT FILE] $_\n" unless $SUMMARY_ONLY;
                        $hits{BOOT_INI}++;
                } elsif (/iissamples/i) {
                        print "[SAMPLES] $_\n" unless $SUMMARY_ONLY;
                        $hits{SAMPLES}++;
                } elsif (/showcode\.asp/i) {
                        print "[SHOWCODE] $_\n" unless $SUMMARY_ONLY;
                        $hits{SHOWCODE}++;
                } elsif (/htr/i) {
                        print "[HTR EXPLOIT] $_\n" unless $SUMMARY_ONLY;
                        $hits{HTR}++;
                } elsif (/\.\./) {
                        print "[\.\. EXPLOIT] $_\n" unless $SUMMARY_ONLY;
                        $hits{DOT_DOT}++;
                }
        }
        close FILEHANDLE;
}
# print the summary results
print "\n\n--------------\nAttack Summary\n--------------\n";
print "$lines lines processed\n\n";
@keys = sort {int $hits{$b} <=> int $hits{$a} } keys %hits;
foreach $key (@keys) {
        $value = $hits{$key};
        $percent = ($value / $lines) * 100;
        printf "%12s = %7d (%0.4f%%) attempts\n",$key,$value,$percent;
}
```

Для применения приведенного выше сценария его необходимо выполнять на отдельном сервере (рабочем месте), не входящим в состав Удостоверяющего Центра. Файлы журнала аудита MS IIS необходимо переносить на сервер анализа журналов с использованием отчуждаемых магнитных носителей.

Рекомендуется регулярно (ежедневно) выполнять анализ журналов аудита MS IIS для определения атак.

8.4.5. Анализ журналов в SQL 2000 Server

В SQL 2000 Server есть два типа журналов:

- журнал приложений (Application) Windows 2000;
- собственный журнал событий.

Собственный журнал событий – это текстовые файлы с наименованием errorlog.NNN, расположенные в каталоге ..\Program Files\Microsoft SQL Server\MSSQL$CPRA\LOG. Имя MSSQL$CPRA является составным и содержит имя (CPRA) именованной установки SQL 2000 Server по умолчанию. NNN – это порядковый номер файла журнала событий.

При указании типа соединения пользователя с сервером возможно указание двух видов:

- Trusted – означает, что учетная запись прошла аутентификацию Windows;
- Non-Trusted – означает, что использовались встроенные средства аутентификации SQL Server.

Для анализа файлов может быть использована команда *findstr*, позволяющей осуществлять поиск подстроки в текстовом файле журналов SQL Server.

Например, findstr /i “login.failed” err*.*

В этом примере будет осуществляться поиск слов login и failed одновременно.

В журнале событий Windows 2000 Server, не зависимо от факта аутентификации, регистрации записи журнала всегда одинаковы. Отличается только их текст. Записи заносятся со следующими значениями полей:

- Источник (Source) – MSSQLServer;
- Категория (Category) – Logon;
- Код события (Event ID) – 17055.

8.5. Защита журналов аудита

8.5.1. Защита журнала модуля политики службы сертификации ЦС

Для обеспечения защиты журналов от преднамеренного искажения необходимо установить соответствующие списки контроля доступа к файлам журналов и регулярно создавать их резервные копии.

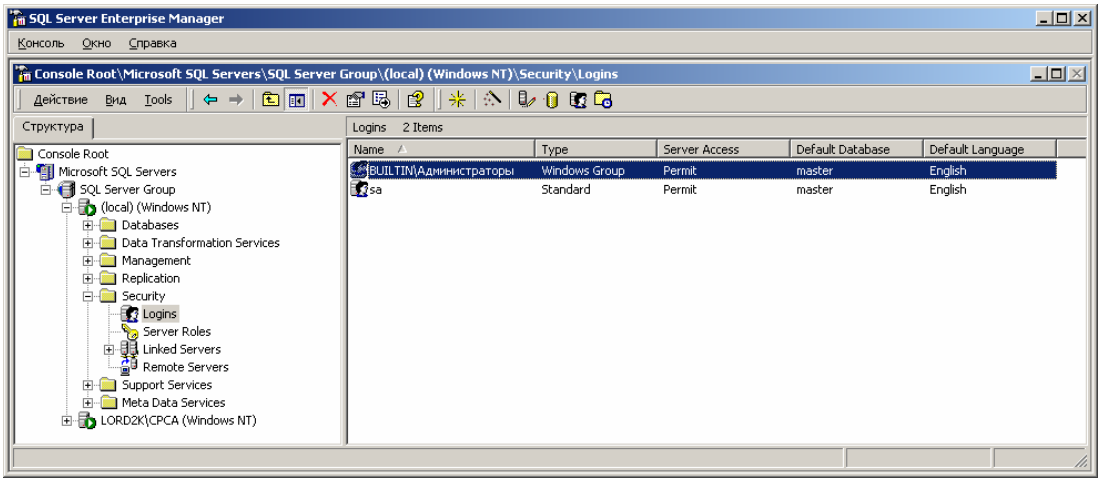
Файл журнала аудита модуля политики службы сертификации ЦС располагается в каталоге %WinDir%\Program Files\Crypto Pro\CA\log (по умолчанию) и имеет наименование CA.log по умолчанию.

8.5.2. Защита журнала ПО Центра Регистрации

Для обеспечения защиты таблиц базы данных Центра Регистрации, образующих журнал аудита, используются средства разграничения доступа SQL 2000 Server совместно со средствами разграничения доступа, предоставляемыми межсетевыми экранами.

Для предустановленного пользователя **dbo** на SQL 2000 Server определить роли **public** и **db_owner** для базы данных Центра Регистрации.

В настройках безопасности (Security) определить учетные записи (Logons) для **локальных администраторов** Windows 2000 Server (**BUILTIN\Администраторы**) и стандартной учетной записи SQL-сервера с наименованием **sa**.



Для этих учетных записей определить роли **public** и **db_owner** для базы данных Центра Регистрации.

С помощью средств разграничения доступа межсетевых экранов запретить удаленное сетевое соединение с SQL-сервером Центра Регистрации для всех компьютеров сети, за исключением сервера Центра Регистрации, на котором исполняются COM+ приложения ЦР.

Такие настройки позволят обеспечить защиту базы данных Центра Регистрации, включая и таблицы журнала аудита, от несанкционированного изменения, со стороны лиц, учетные записи которых не входят в группу администраторов серверов баз данных и Центра Регистрации.

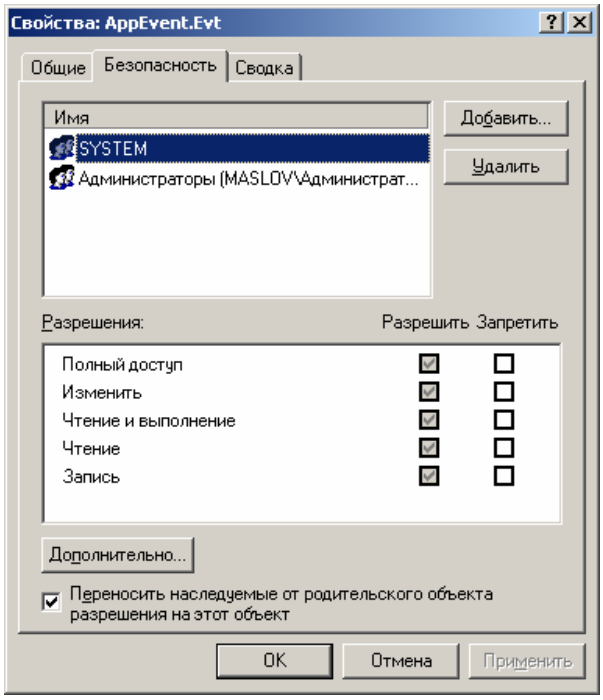
8.5.3. Защита журналов событий MS Windows 2000

Для обеспечения защиты журналов от преднамеренного искажения необходимо установить соответствующие списки контроля доступа к файлам журналов и регулярно создавать их резервные копии.

Журнал событий MS Windows 2000 образуют три файла: AppEvent.evt, SecEvent.evt, SysEvent.evt, расположенные в каталоге \WINNT\System32\config.

Данные файлы по умолчанию имеют следующий список контроля доступа:

- SYSTEM (полный контроль);
- Administrators (полный контроль);



Прочитать или изменить эти регистрационные файлы может только администратор.

8.5.4. Защита журналов событий MS IIS

Для обеспечения защиты журналов от преднамеренного искажения необходимо установить соответствующие списки контроля доступа к файлам журналов и регулярно создавать их резервные копии.

Журналы MS IIS наследуют списки контроля доступа от родительского каталога. Необходимо установить следующие списки контроля доступа к журналам MS IIS:

- Administrators (полный контроль);
- System (полный контроль);

- Everyone (читать/писать/копировать).

Журналы MS IIS хранятся в каталоге %systemroot%\System32\LogFiles.

Эти разрешения гарантируют, что злоумышленники не смогут удалить или очистить журналы, чтобы замести следы взлома.

8.5.5. Защита журналов событий SQL 2000 Server

Для обеспечения защиты журналов от преднамеренного искажения, необходимо установить соответствующие списки контроля доступа к файлам журналов и регулярно создавать их резервные копии.

Файлы журналов SQL Server (errorlog.nnn) имеют следующий список контроля доступа (по умолчанию):

- Administrators (полный контроль);
- Учетная запись, под которой стартует служба MSSQLServer (полный доступ).

Файлы журналов хранятся в каталоге ..\MSSQL\LOG.

9. Смена паролей учетных записей ПК «КриптоПро УЦ»

ПК «КриптоПро УЦ» создает в процессе установки программного обеспечения и использует в своей работе следующие локальные учетные записи:

1. **CPCAComPlusAcct&** - Учетная запись ЦС Крипто-Про УЦ.
2. **CPRAComPlusAcct&** - Учетная запись ЦР Крипто-Про УЦ

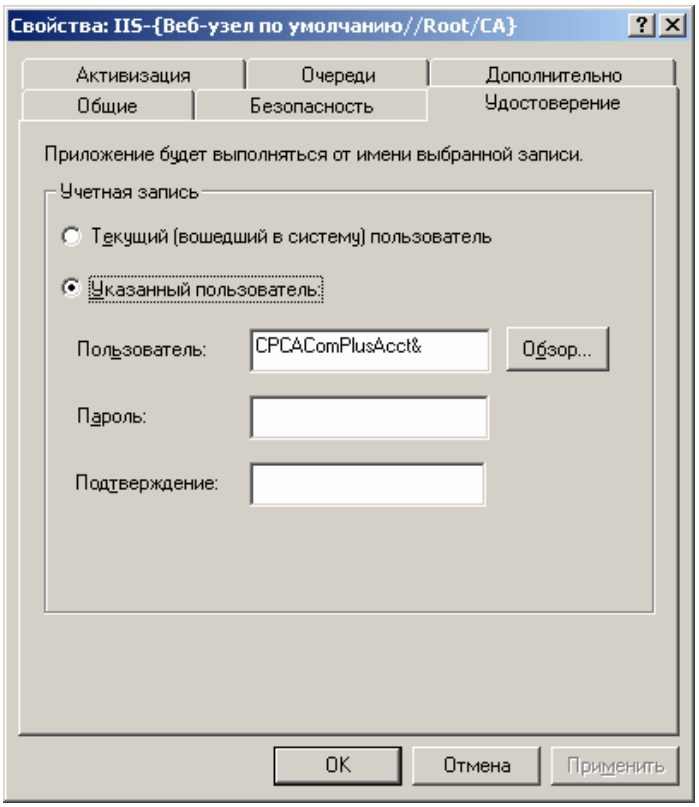
Для данных учетных записей по умолчанию устанавливаются следующие параметры:

- Запретить смену пароля пользователем;
- Срок действия пароля неограничен.

Для смены пароля учетной записи **CPCAComPlusAcct&** необходимо последовательно выполнить следующие действия:

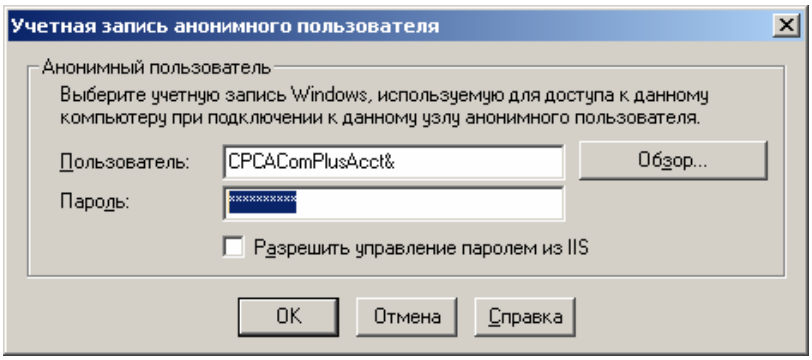
1. Задать новый пароль для локальной учетной записи;
2. В сервисе **Службы компонентов** для приложения COM+ с наименованием **IIS-{Веб-узел по умолчанию//Root/CA}** на вкладке **Удостоверение** ввести и подтвердить новый пароль;

Рисунок 1. Установка пароля учетной записи приложения COM+ IIS-{Веб-узел по умолчанию//Root/CA}



3. В сервисе **Диспетчер служб Интернета** в окне свойств виртуального каталога **CA** на вкладке **Безопасность каталога** в окне свойств и выбора учетной записи для анонимного доступа установить новый пароль для выбранной учетной записи.

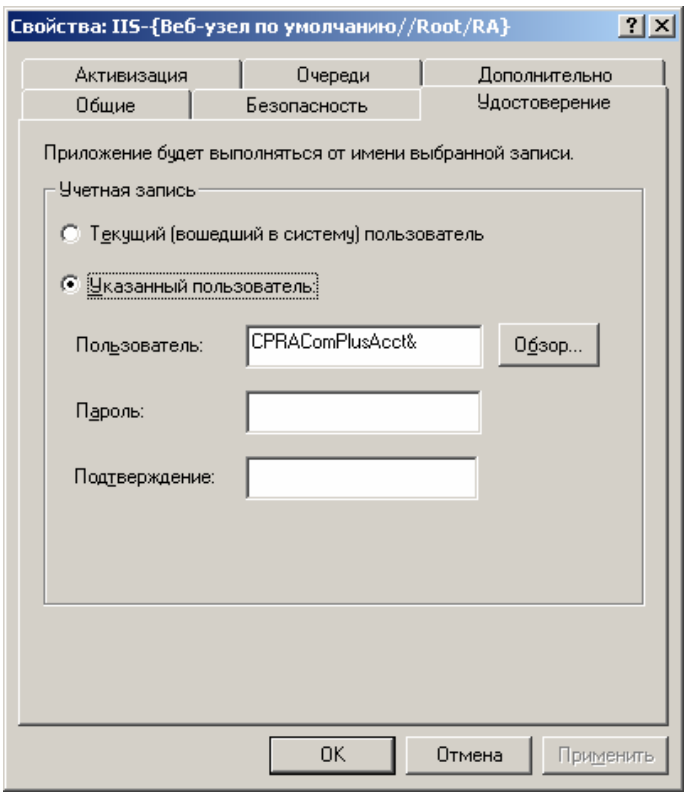
Рисунок 2. Установка пароля учетной записи анонимного доступа виртуального каталога CA



Для смены пароля учетной записи **CPRAComPlusAcct&** необходимо последовательно выполнить следующие действия:

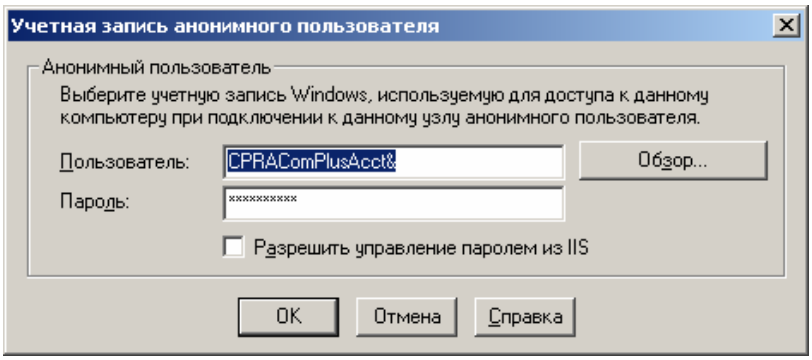
1. Задать новый пароль для локальной учетной записи;
2. В сервисе **Службы компонентов** для приложения COM+ с наименованием **IIS-{Веб-узел по умолчанию//Root/RA}** на вкладке **Удостоверение** ввести и подтвердить новый пароль;

Рисунок 3. Установка пароля учетной записи приложения COM+ IIS-{Веб-узел по умолчанию//Root/RA}



3. В сервисе **Службы компонентов** для приложения COM+ с наименованием **IIS-{Веб-узел по умолчанию//Root/UI}** на вкладке **Удостоверение** ввести и подтвердить новый пароль;
4. В сервисе **Диспетчер служб Интернета** в окне свойств виртуальных каталогов **RA** и **UI** на вкладке **Безопасность каталога** в окне свойств и выбора учетной записи для анонимного доступа установить новый пароль для выбранной учетной записи.

Рисунок 4. Установка пароля учетной записи анонимного доступа виртуальных каталогов



Смена паролей учетных записей не по приведенной выше схеме приведет к неработоспособности ПК «КриптоПро УЦ» в целом.

10. Требования к серверным и рабочим помещениям удостоверяющего центра

Настоящие требования к серверным и рабочим помещениям удостоверяющего центра носят рекомендуемый характер и не являются обязательными по выполнению в части количества выделенных рабочих помещений.

10.1. Серверное помещение

Сервера Центра Сертификации, Центра Регистрации Удостоверяющего Центра и телекоммуникационное оборудование должны быть размещены в выделенном помещении (далее по тексту – серверное помещение Удостоверяющего Центра).

Серверное помещение Удостоверяющего Центра должно быть оборудовано системой контроля доступа с идентификацией по карте.

Идентификационные карты для доступа в серверное помещение выдаются сотрудникам из состава Службы Безопасности и Технической Службы УЦ по приказу руководителя Удостоверяющего Центра.

Серверное помещение Удостоверяющего Центра должно быть оборудовано исполнительным устройством системы контроля доступа электромеханического типа.

Технические средства Удостоверяющего Центра должны быть подключены к общегородской сети электроснабжения.

Электрические сети и электрооборудование, используемые в Удостоверяющем Центре, должны отвечать требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

Серверное помещение должно быть оборудовано средствами вентиляции и кондиционирования воздуха, обеспечивающих соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

Серверное помещение Удостоверяющего Центра должно быть оборудовано системой автоматического пожаротушения, пожарной сигнализации и дымоудаления.

Пожарная безопасность помещений Удостоверяющего Центра обеспечивается в соответствии с нормами и требованиями СНиП по классу Ф3.5, устанавливаемыми законодательством Российской Федерации.

Помещения и технические средства, расположенные в нем, должны пройти проверку на отсутствие в них электронных устройств перехвата информации (закладок).

10.2. Рабочие помещения

Рабочие помещения Удостоверяющего Центра выделяются по схеме организации рабочих мест персонала Удостоверяющего Центра.

Рабочие помещения Удостоверяющего Центра должны оборудоваться механическими замками.

Ключи механических замков рабочих помещений Удостоверяющего Центра выдаются сотрудникам Удостоверяющего Центра по распоряжению руководителя Административной Службы УЦ на основании схемы организации рабочих мест персонала.

Технические средства Удостоверяющего Центра, размещаемые в рабочих помещениях, подключаются к общегородской сети электроснабжения.

Электрические сети и электрооборудование, используемые в рабочих помещениях Удостоверяющего Центра, должны отвечать требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

Рабочие помещения Удостоверяющего Центра должны быть оборудованы средствами вентиляции и кондиционирования воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

Пожарная безопасность рабочих помещений Удостоверяющего Центра обеспечивается в соответствии с нормами и требованиями СНиП по классу Ф3.5, устанавливаемыми законодательством Российской Федерации.

Рабочие помещения Удостоверяющего Центра включают в себя следующие отдельные помещения:

- помещение административного персонала;
- помещение персонала по обеспечению безопасности;
- помещение персонала по обеспечению регистрации;
- помещение технического персонала и кладовая.

Помещение персонала по обеспечению регистрации должно быть разделено на две части (перегорожено барьером): в одной части располагается рабочие места операторов Центра Регистрации, другая предназначена для приема посетителей.

Во внерабочее время все рабочие помещения должны быть опечатаны.

10.3. Архивохранилище

Архивные документы должны хранится в специально оборудованном помещении-архивохранилище, обеспечивающем режим хранения архивных документов, устанавливаемый законодательством Российской Федерации.

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводи-тельного документа и дата	Подпись	Дата
Изм.	изменен-ных	Замененных	новых	аннулированных					