МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

И.В. Ананченко, О.В. Алейникова, Ю.М. Шапаренко

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ
Часть 2. АППАРАТНЫЕ USB-ТОКЕНЫ И СМАРТ-КАРТЫ JaCarta. СРЕДСТВО ЗАЩИТЫ JaCarta SecurLogon

Учебно-методическое пособие по дисциплине
«Техническая защита информации»
Направление подготовки 10.05.02 Информационная безопасность
телекоммуникационных систем

Санкт-Петербург
РГГМУ
2020

УДК 004.056(072.8+075.8)
ББК 32.972.5я73

А64 **Ананченко И.В., Алейникова О.В., Шапаренко Ю.М.** Информационная безопасность телекоммуникационных систем. Часть 2. Аппаратные USB-токены и смарт-карты JaCarta. Средства защиты JaCarta SecurLogon. – СПб.: РГГМУ, 2020. – 28 с.

В учебно-методическом пособии рассматриваются вопросы исследования аппаратных USB-токенов и смарт-карт JaCarta (установка и администрирование), а также развертывание и использование средства защиты JaCarta SecurLogon. Работа ориентирована на обретение студентами навыков установки и эксплуатации программно-аппаратного решения, предназначенного для кардинального решения проблемы «слабых» паролей при работе на компьютерах под управлением Microsoft Windows. Материал пособия соответствует содержанию дисциплины «Техническая защита информации» государственных образовательных стандартов ФГОС 3+. Позволяют формировать общепрофессиональные компетенции (ПК-2,11,12) по направлению подготовки специалистов 10.05.02 «Информационная безопасность телекоммуникационных систем».

Учебно-методическое пособие предназначено для специалистов, магистров и аспирантов высших учебных заведений, обучающихся по направлению 10.00.00 – Информационная безопасность.

© И.В. Ананченко, О.В. Алейникова, Ю.М. Шапаренко, 2020
© Российский государственный гидрометеорологический университет, 2020

Введение

Развитие инфокоммуникационных систем и компьютерных технологий сопровождается появлением новых видов угроз информационной безопасности ТКС и вынуждает наращивать усилия по технической защите информации [1].

В этих условиях IT-специалисты по защите информации должны иметь навыки установки и эксплуатации непрерывно обновляющихся программно-аппаратных решений, предназначенных для предотвращения несанкционированного доступа к информации [2].

При работе на компьютерах под управлением различных операционных систем есть проблема «слабых» паролей. Существует множество вариантов паролирования и предложений соответствующих аппаратно-программных средств. Для обучения авторизации пользователей в операционных системах , например , в ОС Windows, могут быть использованы программное обеспечение JaCarta SecurLogon и аппаратные USB-токены и смарт-карты JaCarta.

JaCarta SecurLogon позволяет повысить уровень безопасности при входе на локальный компьютер и в корпоративную сеть под управлением ОС Windows за счёт простого и быстрого перехода от авторизации по логину и паролю к двухфакторной аутентификации на основе электронного ключа. При этом отсутствует необходимость настройки Active Directory, внедрения PKI-инфраструктуры и создания собственного Удостоверяющего центра для выпуска сертификатов пользователей. При использовании JaCarta SecurLogon конечный пользователь не будет вводить с клавиатуры пароль Windows, что исключает возможность подсматривания или перехвата пароля злоумышленником.

Лабораторная работа 1

Цель: обретение навыков установки программного обеспечения (ПО) JaCarta SecurLogon.

Теория: JaCarta SecurLogon – сертифицированное программно-аппаратное решение, позволяющее осуществить простой и быстрый переход от однофакторной аутентификации на основе пары логин-пароль к двухфакторной аутентификации при входе в операционную систему и доступе к сетевым ресурсам за счёт использования USB-токенов и смарт-карт. Для функционирования JaCarta SecurLogon не нужно закупать дорогостоящее серверное оборудование для развёртывания Active Directory и собственного Удостоверяющего центра для выпуска цифровых сертификатов. Вместо них JaCarta SecurLogon генерирует сложные пароли (до 63-х символов), которые записываются в USB-токен или смарт-карту. При этом такие пароли могут быть неизвестны и не видны самим пользователям, им остаётся лишь запомнить свой простой и короткий PIN-код. Поддержка биометрической аутентификации позволяет заменить ввод PIN-кода сканированием отпечатка пальца.

Порядок выполнения работы:

1) Сначала устанавливается ПО и выбирается режим установки (выборочная) компонентов (рис. 1).

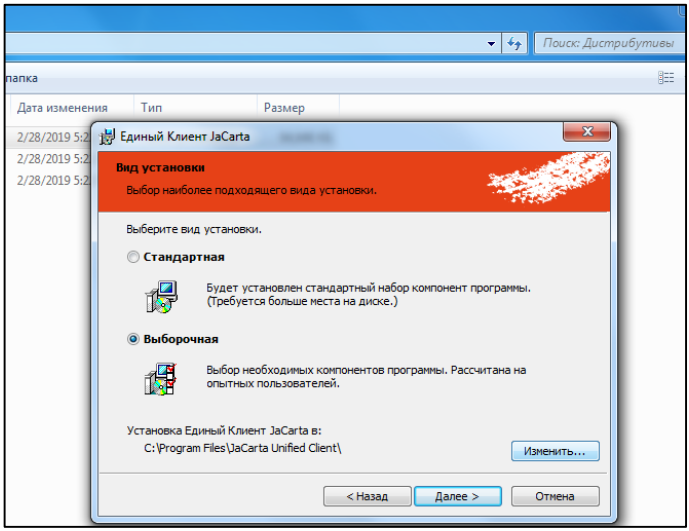


Рис. 1. Выбор режима установки

Если выбраны «Единый Клиент JaCarta», «JaCarta SecurLogon», «Драйверы», исключены (x) «JaCarta WebPass Tool», «JaCarta АРМ УЦ» и поддержка системы биометрии (рис. 2), то можно запустить процесс установки (рис. 3).

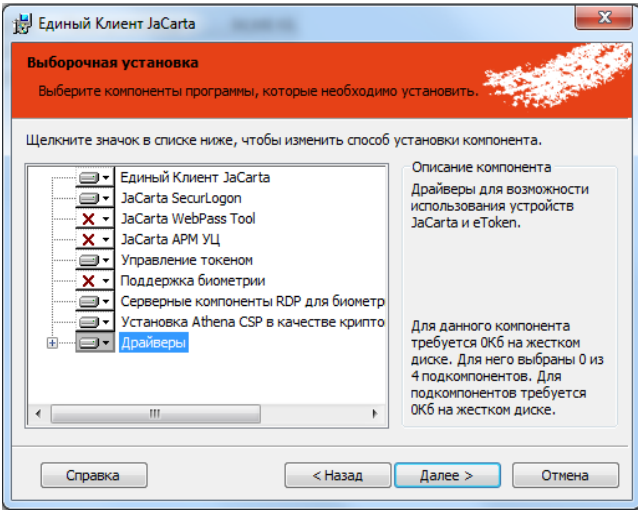


Рис. 2. Выбор компонентов установки

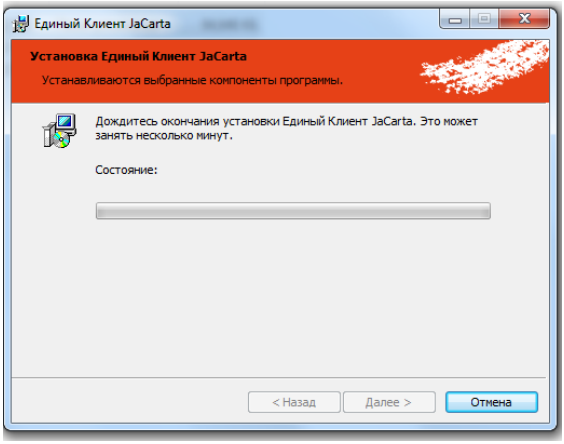


Рис. 3. Процесс установки

2) Далее настраиваются профили. После подключения кардридера с картой Единый клиент JaCarta ПО активируется. Появляется возможность настройки профиля (рис. 4).

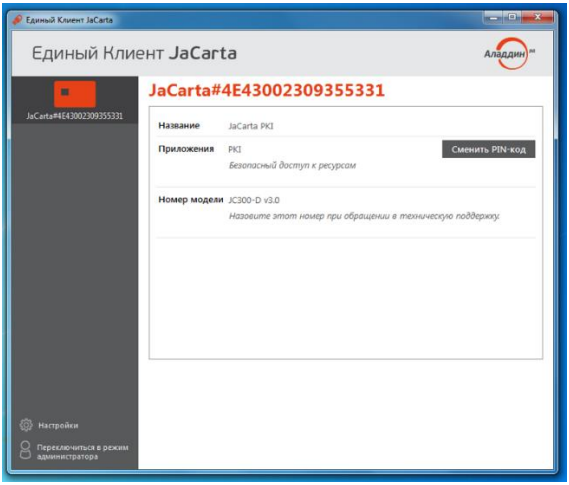


Рис. 4. ПО после подключения картридера

Выполняется вход в режим администратора для установки лицензии и создается профиль. Файл лицензии выбирается на жестком диске компьютера, добавляется профиль timod, указываются пароль и PIN – 11111111 (рис. 5).

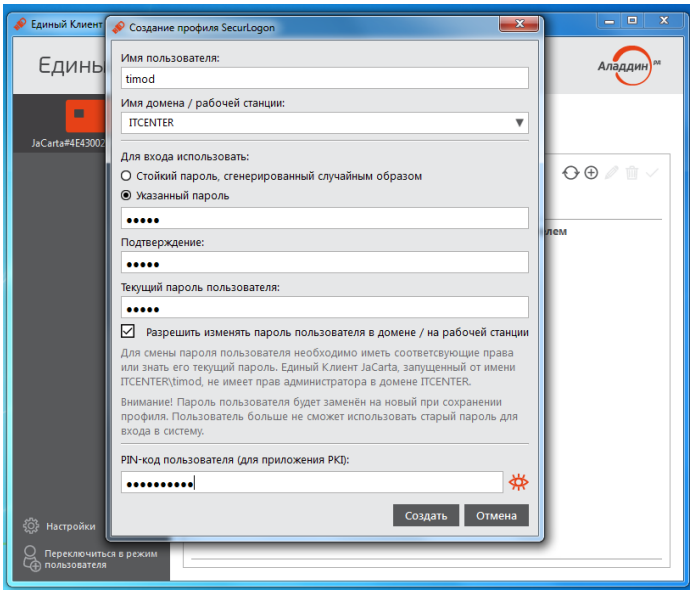


Рис. 5. Создание профиля

Список пользователей представлен на рис. 6.

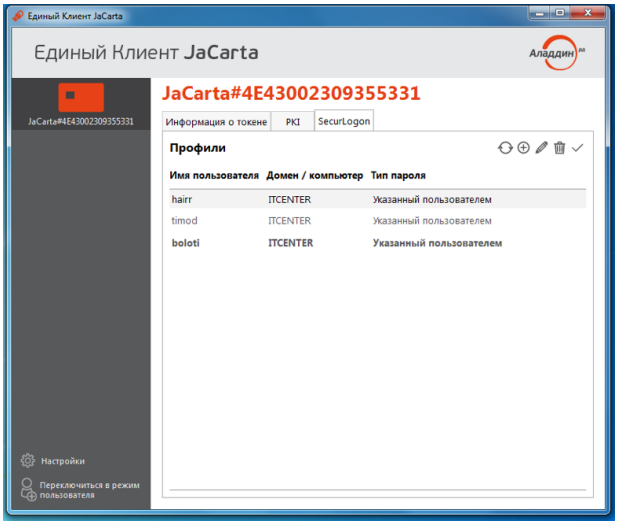


Рис. 6. Список пользователей

3) Выполняется вход в учетную запись (рис. 7).

Рис. 7. Вход в учетную запись

4) Смена PIN-кода электронного ключа.

При получении электронного ключа на руки настоятельно рекомендуется осуществить смену PIN-кода пользователя.

После установки ПО Единый клиент JaCarta пользователь имеет возможность сменить PIN-код электронного ключа двумя способами:

1. До входа в ОС с помощью запуска модуля "Управление токеном" (рис. 8).
2. После входа в ОС с помощью запуска ПО Единый клиент JaCarta (рис. 9).

Для смены PIN-кода необходимо знать текущий PIN-код электронного ключа.

Значения PIN-кодов, используемых для различных моделей электронных ключей по умолчанию, приведены в таблице 1.

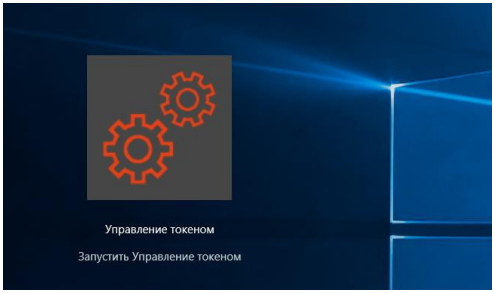


Рис. 8. Смена PIN-кода до входа в ОС

Таблица 1. Значения PIN-кодов для электронных ключей

Параметры	Модели электронных ключей:				
	eToken PRO eToken PRO (Java) eToken NG-FLASH eToken NG-FLASH (Java) eToken NG-OTP eToken NG-OTP (Java) JaCarta PKI	JaCarta PKI JaCarta PKI/Flash JaCarta PKI/BIO	JaCarta ГОСТ/Flash JaCarta ГОСТ eToken ГОСТ	JaCarta LT	JaCarta CryptoPro
Приложение	PKI	PKI и PKI/BIO	ГОСТ	STORAGE	ФКН
PIN-код пользователя по умолчанию	1234567890	11111111	Не установлен	1234567890	Нет
Поведение ключа при разблокировке PIN-кода пользователя	Во время разблокировки администратор задаёт новый PIN-код пользователя		Разблокировка сбрасывает счётчик неверных попыток доступа – PIN-код пользователя при этом остаётся неизменным		Нет
Можно разблокировать PIN-код пользователя в удалённом режиме	Да	Да	Нет	Нет	Нет
Администратор может сменить установленный PIN-код пользователя без инициализации	Да	Да	Нет	Нет	Нет

Рис. 9. Смена PIN-кода после входа в ОС

После нажатия кнопки "**Сменить PIN-код**" должно появиться окно, показанное на рис. 10, в котором необходимо ввести текущий PIN-код, новый PIN-код и подтвердить PIN-код, введя его еще раз.

Если все данные введены правильно, то после нажатия кнопки "**Выполнить**" должно окно об спешной смене PIN-кода.

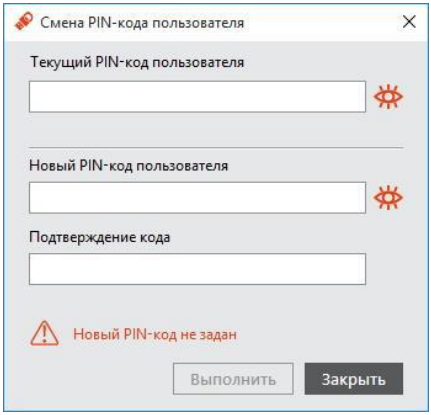


Рис. 10. Окно смены PIN-кода

Регистрация результатов работы

Выполнение работы осуществляется в соответствии с рекомендованным выше порядком после получения экземпляра карты. В отчет вставляются скриншоты, подтверждающие работоспособность ПО и осуществление входа в учетную запись. Проверяется возможность применять сложные пароли и отсутствие необходимости их вводить

вручную при автоматической генерации надежных паролей.

Выводы должны подтверждать получение навыков установки и администрирования ПО «JaCarta SecurLogon», оценки достоинств и недостатков данного ПО.

Лабораторная работа 2

Цель: обретение навыков администрирования ПО JaCarta SecurLogon.

Теория: Единый клиент JaCarta может работать в двух режимах:

1. Режим пользователя – позволяет просматривать краткие сведения о подсоединённых электронных ключах и предоставляет доступ к базовым операциям с электронными ключами.
2. Режим администрирования – позволяет просматривать полные сведения о подсоединённых электронных ключах и предоставляет доступ ко всем операциям с электронными ключами.

Для переключения в режим администрирования необходимо в окне Единого клиента JaCarta кликнуть левой кнопкой мыши по надписи "**Переключиться в режим администрирования**" (рис. 11).

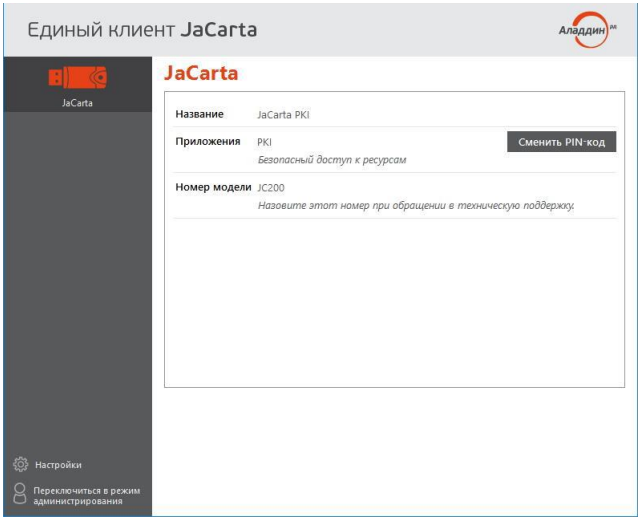


Рис. 11. Переключение в режим администрирования

Для переключения в режим пользователя необходимо в окне Единого клиента JaCarta кликнуть левой кнопкой мыши по надписи "**Переключиться в режим пользователя**" (рис. 12).

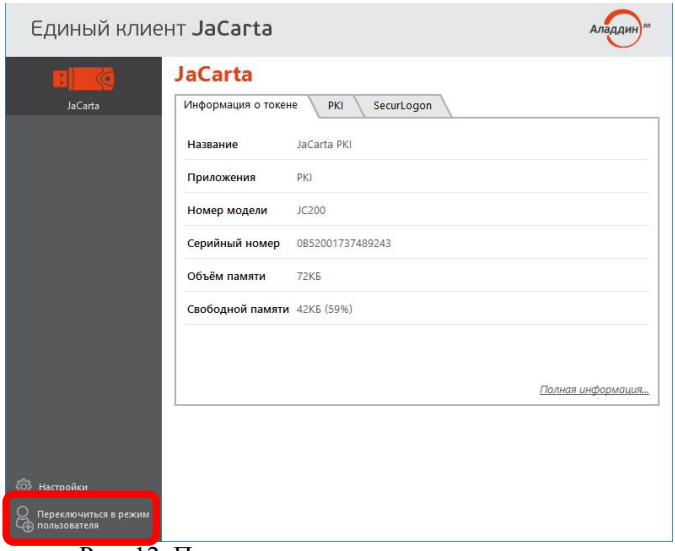


Рис. 12. Переключение в режим пользователя

Порядок выполнения работы:

1) Установка лицензии

Установить лицензию JaCarta SecurLogon можно двумя способами:

1. В режиме пользователя: через меню Настройки в окне Единого клиента JaCarta;
2. В режиме администрирования: через вкладку SecurLogon в окне Единого клиента JaCarta.

Чтобы установить лицензию, необходимо обладать правами администратора.

В случае установки лицензии через вкладку SecurLogon в окне Единого клиента JaCarta необходимо подсоединить электронный ключ к компьютеру.

В случае установки лицензии через меню Настройки в окне Единого клиента JaCarta подсоединять электронный ключ к компьютеру не обязательно.

Установку лицензии через меню Настройки производить в следующей последовательности:

1) Запустить Единый клиент JaCarta и кликнуть левой кнопкой мыши по надписи **Настройки** в левом нижнем углу окна Единого клиента JaCarta (рис. 13).

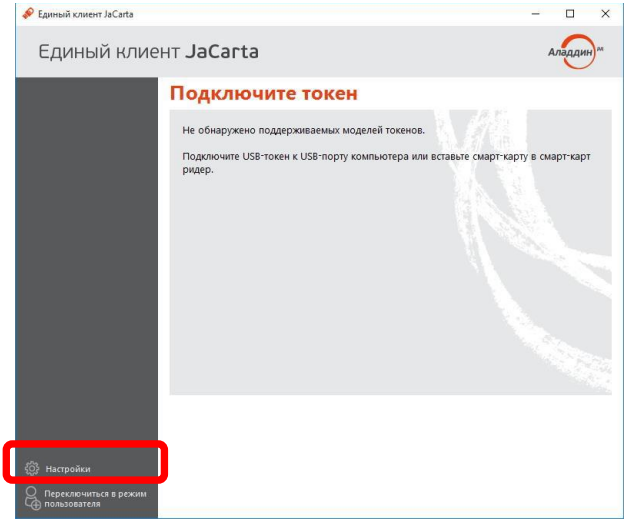


Рис. 13. Переключение в режим Настойки

2) В отобразившемся окне выбрать вкладку SecurLogon и нажать кнопку "**Установить лицензию SecurLogon…**" (рис. 14).

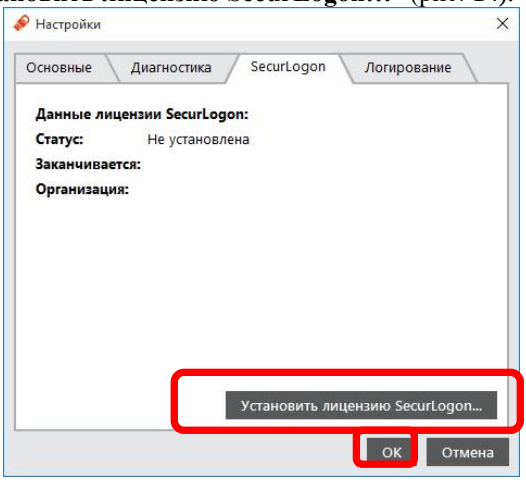


Рис. 14. Установка лицензии

3) В отобразившемся окне необходимо указать путь к файлу лицензии и нажать кнопку "**Открыть**".

4) После установки лицензии в отобразившемся окне нажать кнопку **ОК** (рис. 14).

Установку лицензии через вкладку SecurLogon производить в следующей последовательности:

1) Подключить электронный ключ к компьютеру и запустить Единый клиент JaCarta, после чего переключиться в режим администратора, перейти на вкладку SecurLogon и в статусе лицензии нажать ссылку "установить" (рис. 15).

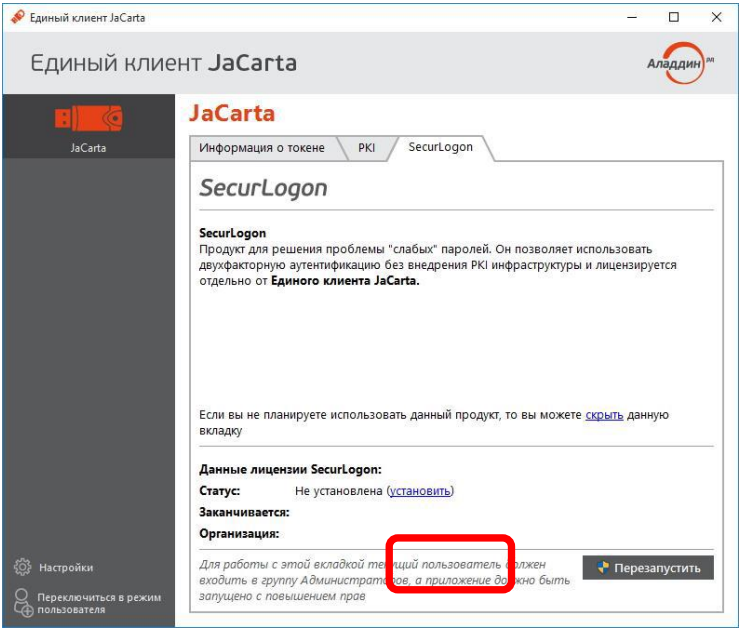


Рис. 15. Установка лицензии через вкладку SecurLogon

Далее в отобразившемся окне необходимо указать путь к файлу лицензии и нажать кнопку "**Открыть**".

При успешном завершении операции вкладка SecurLogon примет следующий вид (рис. 16).

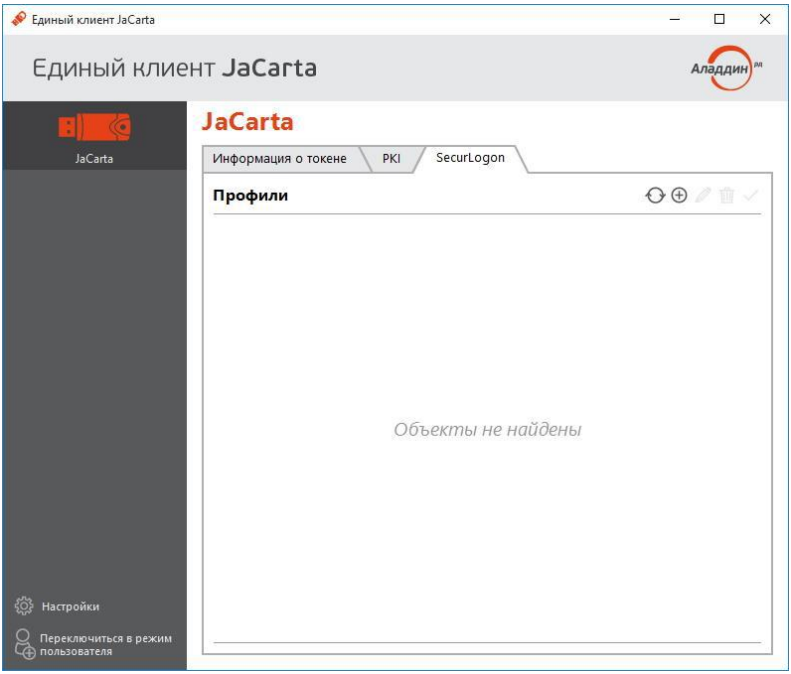


Рис. 16. Окно завершения операции установки лицензии

2) Настройка работы. Операции с профилями.

Чтобы создать профиль JaCarta SecurLogon, необходимо выполнить следующие действия:

1) Подсоединить электронный ключ, на котором требуется создать профиль JaCarta SecurLogon, к компьютеру и запустить Единый клиент JaCarta;

2) Переключиться в режим администратора и перейти на вкладку SecurLogon (рис. 17).

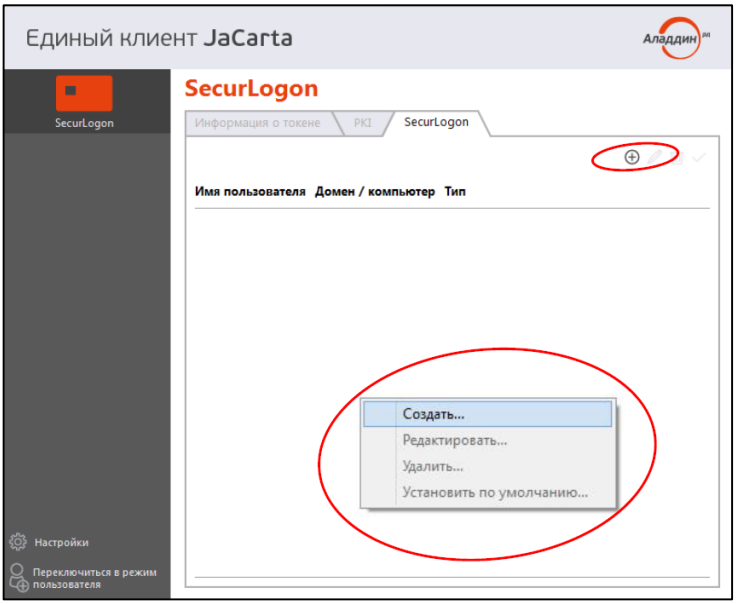


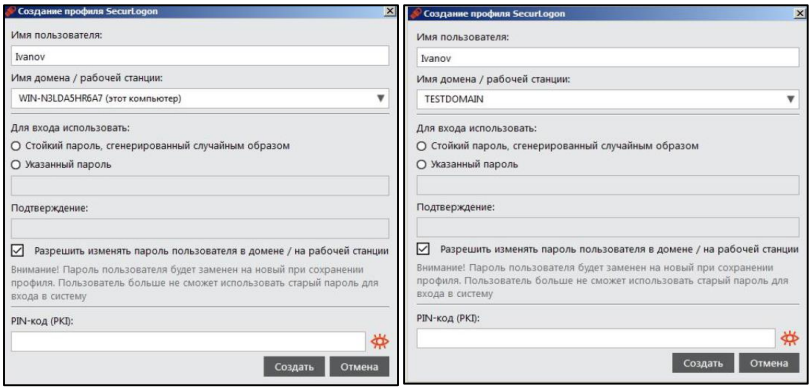
Рис. 17. Вкладка SecurLogon

3) Нажать на значок ⊕ или нажать правой кнопкой мыши в центральной части окна и в контекстном меню выбрать "**Создать…**" (рис. 17);

В зависимости от того, создаётся ли профиль JaCarta SecurLogon для локальной учётной записи или для учётной записи в домене Windows окно создания профиля может быть двух видов (рис. 18а) – для локальной учетной записи и (рис. 18б) – для учетной записи в домене Windows.

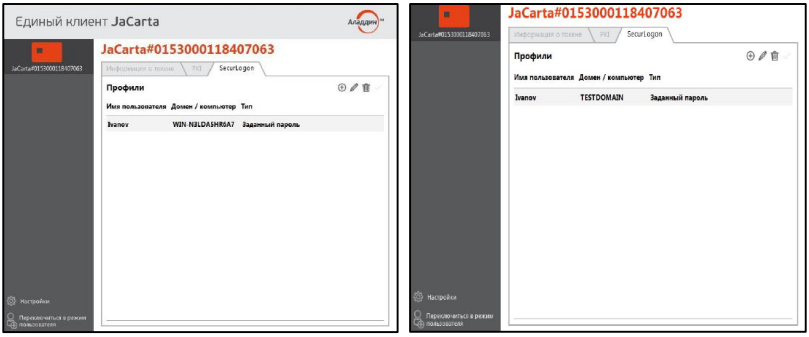
4) В появившемся окне (рис. 18) следует выбрать, какой тип пароля будет использоваться для входа, ввести PIN-код электронного ключа и нажать кнопку "**Создать**".

5) Созданный профиль должен отобразиться в окне Единого клиента JaCarta на вкладке SecurLogon (рис. 19а) – для локальной учетной записи и (рис. 19б) – для учетной записи в домене Windows.



а) б)

Рис. 18. Окно создания профиля:
а) для локальной учетной записи б) для учетной записи в домене Windows



а) б)

Рис. 19. Окно созданного профиля:
а) для локальной учетной записи б) для учетной записи в домене Windows

Если в настройках административного шаблона JaCarta SecurLogon параметр **AllowProfileManagement** отключен, то создание профилей будет заблокировано.

Если на электронном ключе уже есть профиль текущего пользователя, а в настройках административного шаблона JaCarta SecurLogon параметр **SingleProfileOnly** отключен, то создание других профилей будет заблокировано.

Если в настройках административного шаблона JaCarta SecurLogon параметр **CanCreateProfilesForOtherUsers** отключен, то при создании

нового профиля изменение имени текущего пользователя будет заблокировано.

JaCarta SecurLogon позволяет установить профиль по умолчанию – т.е. такой профиль будет отображаться первым при входе в систему.

Чтобы установить профиль по умолчанию, необходимо выполнить следующие действия:

1) Подсоединить электронный ключ, на котором находится профиль JaCarta SecurLogon, к компьютеру.

2) Запустить Единый клиент JaCarta, переключиться в режим администратора и перейти на вкладку SecurLogon.

3) Левой кнопкой мыши выбрать профиль, который необходимо сделать профилем по умолчанию.

4) В окне Единого клиента JaCarta нажать на значке ✓ (рис. 20) или нажать правой кнопкой мыши на строке с выбранным профилем и из контекстного меню выбрать "**Установить по умолчанию…**".

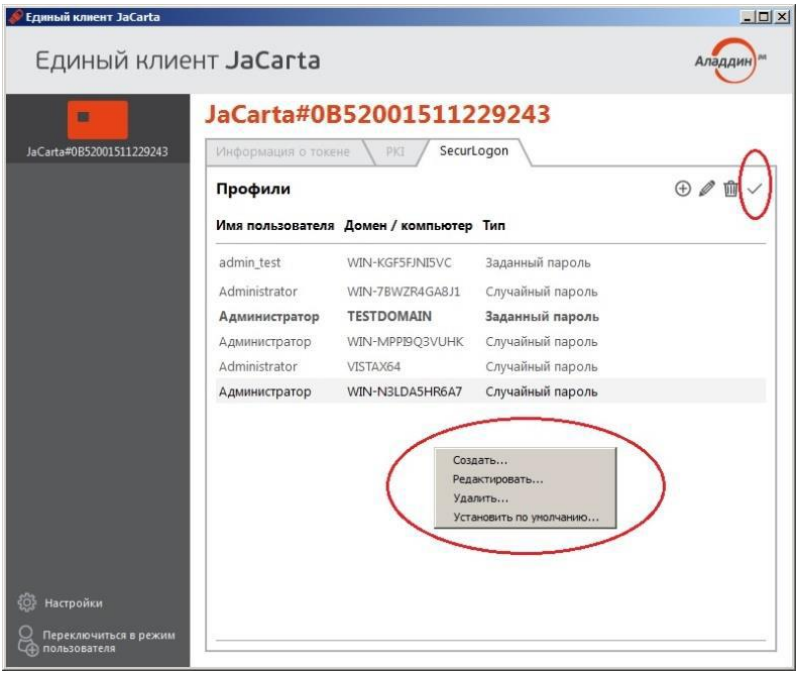


Рис. 20. Окно Единого клиента JaCarta

5) Далее в отобразившемся окне (рис. 21) ввести PIN-код и нажать **ОК**.

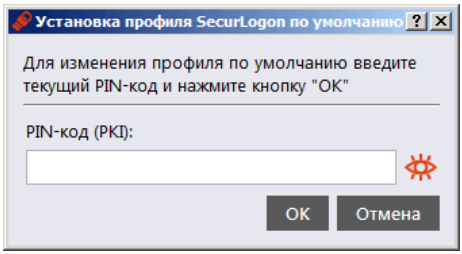


Рис. 21. Окно установки профиля по умолчанию

6) Выбранный ранее профиль в окне Единого клиента JaCarta должен стать профилем по умолчанию, т.е. быть выделен жирным шрифтом среди других профилей (рис. 22).

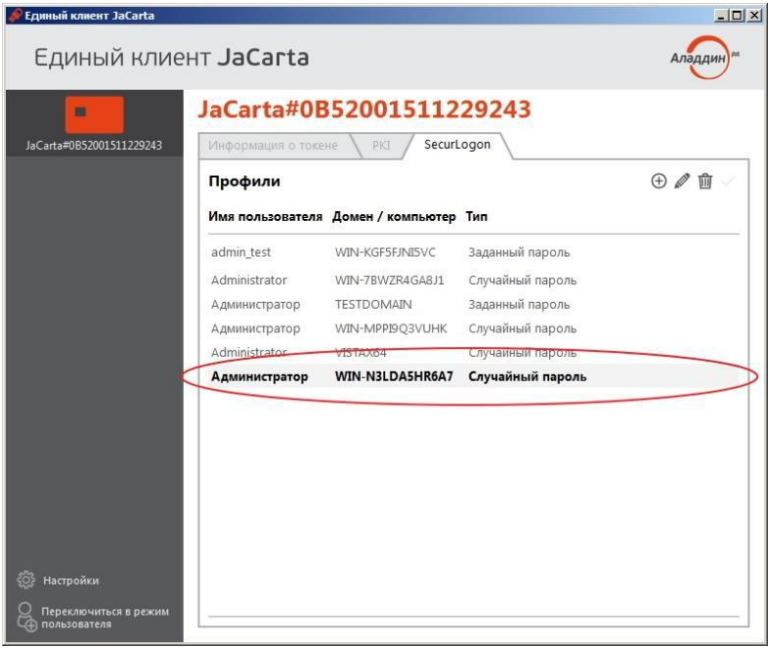


Рис. 22. Установленный профиль по умолчанию

Чтобы отредактировать профиль JaCarta SecurLogon, необходимо выполнить следующие действия:

1) Подсоединить электронный ключ с записанным профилем JaCarta SecurLogon к компьютеру.

2) Запустить Единый клиент JaCarta, переключиться в режим администратора и перейти на вкладку SecurLogon.

3) Левой кнопки мыши выбрать профиль, который необходимо изменить.

4) Нажать на значок ✎ (рис. 23) или нажать правой кнопкой мыши на выбранном профиле и из контекстного меню выбрать "**Редактировать…**".

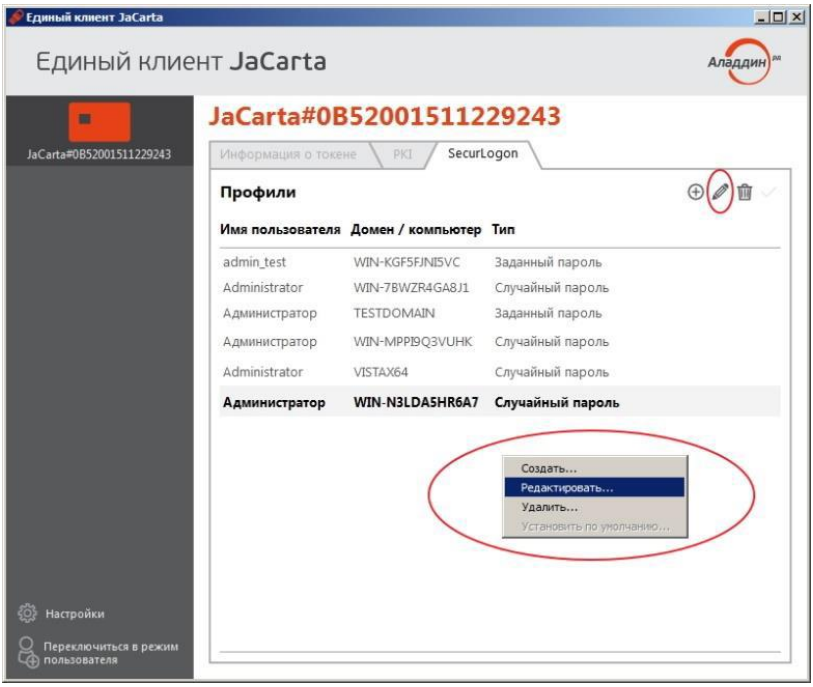


Рис. 23. Редактирование профиля

5) Далее в отобразившемся окне (рис. 24) выполнить необходимые изменения и нажать "**Сохранить**".

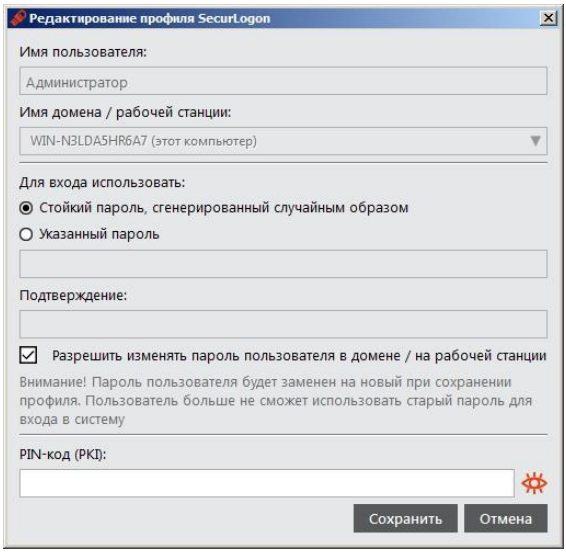


Рис. 24. Внесение изменений в профиль

Чтобы удалить профиль JaCarta SecurLogon из памяти электронного ключа, необходимо выполнить следующие действия:

1) Подсоединить электронный ключ с записанным профилем JaCarta SecurLogon к компьютеру.

2) Запустить Единый клиент JaCarta, переключиться в режим администратора и перейти на вкладку SecurLogon.

3) Нажатием левой кнопки мыши выбрать профиль, который необходимо удалить.

4) Нажать на значок 🗑 или нажать правой кнопкой мыши на выбранном профиле и из контекстного меню выбрать "**Удалить…**" (рис. 25).

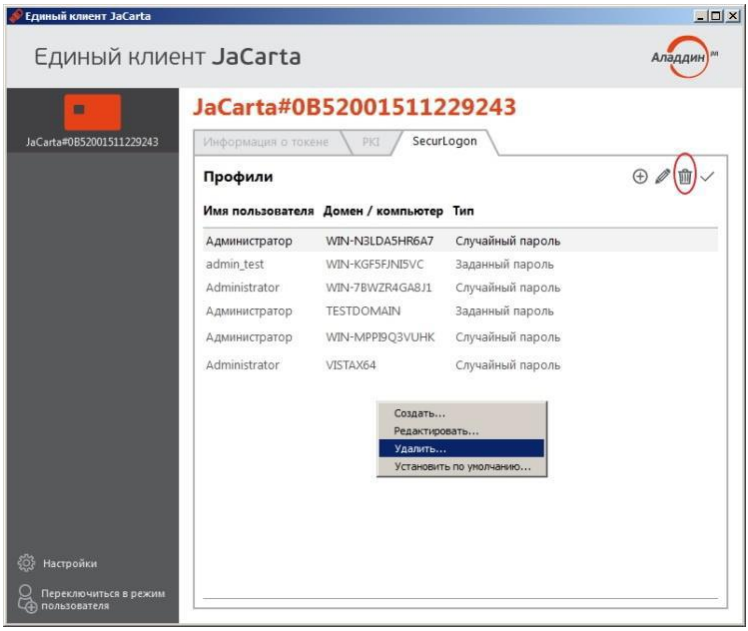


Рис. 25. Удаление профиля

Дальнейшая процедура различается в зависимости от типа пароля, установленного при создании профиля JaCarta SecurLogon (указанный пароль (вводимый вручную) или стойкий пароль, сгенерированный случайным образом).

В случае, если при создании профиля был выбран "Указанный пароль", то в отобразившемся окне следует ввести PIN-код электронного ключа и нажать кнопку "**Удалить**" (рис. 26).

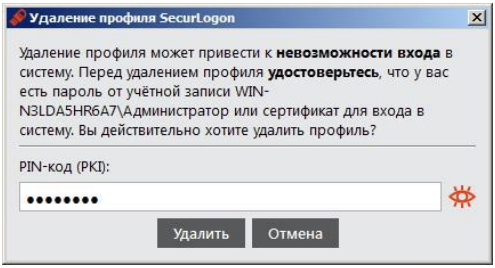


Рис. 26. Удаление профиля

В случае, если при создании профиля был выбран "Стойкий пароль, сгенерированный случайным образом", то в отобразившемся окне следует ввести новый пароль (пароль, который будет назначен учетной записи пользователя после удаления профиля JaCarta SecurLogon) и повторно подтвердить введенный пароль, после чего ввести PIN-код электронного ключа и нажать кнопку "**Удалить**" (см. рис. 27).

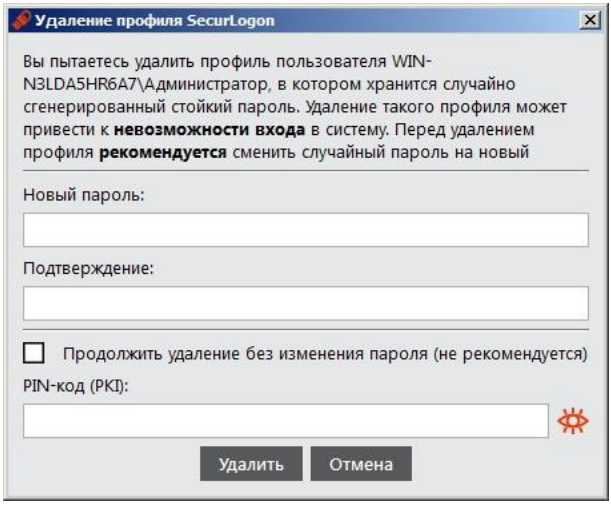


Рис. 27. Удаление профиля при стойком пароле

Если установить флажок в опции "Продолжить удаление без изменения пароля (не рекомендуется)", то вводить новый пароль и его подтверждение не требуется, однако, после удаления профиля JaCarta SecurLogon для доступа к учётной записи пользователя сохранится случайный пароль, сгенерированный при создании профиля JaCarta SecurLogon. Не рекомендуется устанавливать этот флажок, т.к. в этом случае пароль для доступа к учётной записи пользователя останется неизвестным, а доступ будет невозможен.

Настройка административного шаблона.

Перечисленные ниже действия следует выполнять на сервере, являющимся контроллером домена или и на компьютере, на которым установлены средства управлениям контроллером домена.

Чтобы запустить административный шаблон JaCarta SecurLogon и отобразить его настройки необходимо выполнить следующие действия:

1) Нажать на клавиатуре сочетание клавиш **Win+R**, в появившемся окне набрать **gpmc.msc** и нажать **ОК** (см. рис. 28).

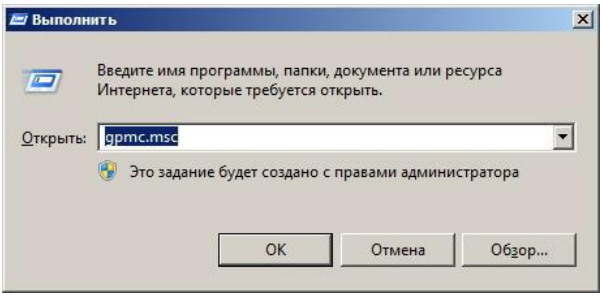


Рис. 28. Запуск административного шаблона

2) В появившемся окне (рис. 29) следует выбрать **Лес => Домены => имя_домена**, далее нажать правой кнопкой мыши на пункте **Default Domain Policy** (Политика домена по умолчанию) и из появившегося контекстного меню выбрать опцию "**Изменить…**".

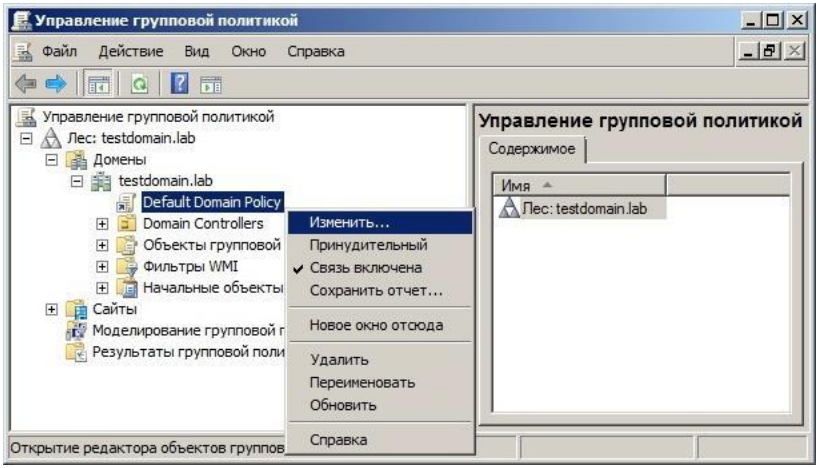


Рис. 29. Окно управления групповой политикой

3) В появившемся окне (рис. 30) следует выбрать **Конфигурация компьютера => Политики => Административные шаблоны => JaCarta SecurLogon**.

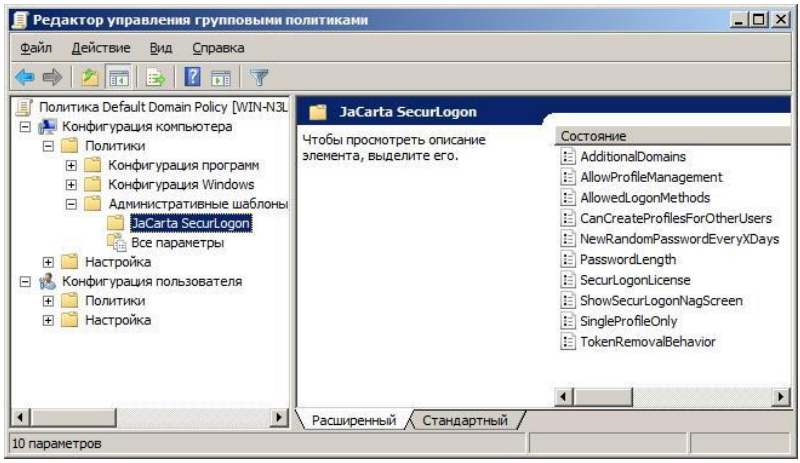


Рис. 30. Окно редактора управления групповыми политиками

4) Редактирование административного шаблона JaCarta SecurLogon производится путем изменения значения параметров политик, входящих в шаблон.

Описание настроек административного шаблона JaCarta SecurLogon с указанием значений параметров политик по умолчанию приведены в Приложении А.

Чтобы запустить административный шаблон JaCarta SecurLogon и отобразить его настройки необходимо выполнить следующие действия:

1) Нажать на клавиатуре сочетание клавиш **Win+R**, в появившемся окне набрать **gpedit.msc** и нажать **ОК** (рис. 31).

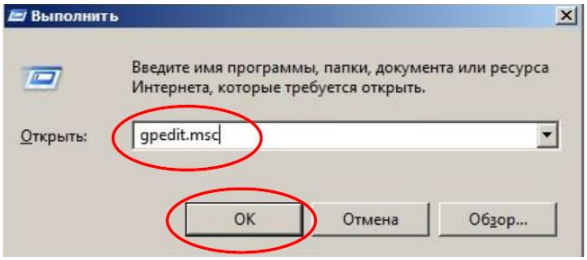


Рис. 31. Запуск административного шаблона JaCarta SecurLogon

2) В появившемся окне выбрать **Конфигурация компьютера => Административные шаблоны => Компоненты Windows => JaCarta SecurLogon** (рис. 32).

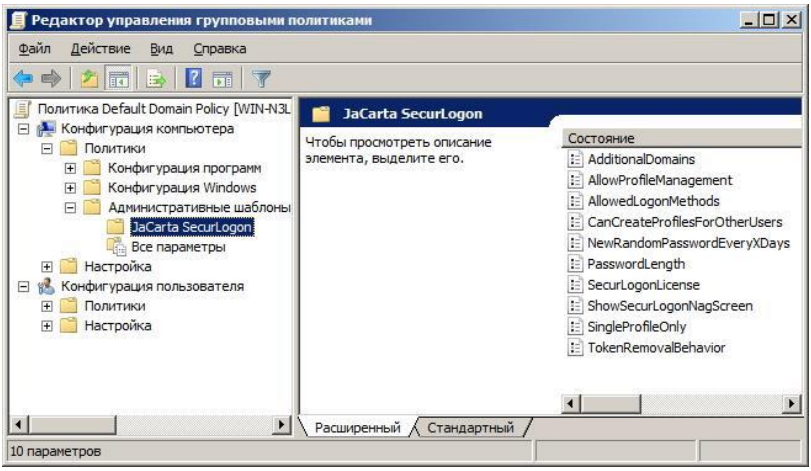


Рис. 32. Окно редактора управления групповыми политиками

3) Редактирование административного шаблона JaCarta SecurLogon производится путем изменения значения параметров политик, входящих в шаблон.

В случае, если пользователь введет несколько раз подряд неправильный PIN-код, то его электронный ключ будет заблокирован.

Регистрация результатов работы

Выполнение работы осуществляется в соответствии с рекомендованным выше порядком после получения экземпляра токена. В отчет вставляются скриншоты, подтверждающие работоспособность ПО и установки лицензии, настройки работы, операции с профилями и шаблонами.

Выводы должны подтверждать получение навыков администрирования ПО «JaCarta SecurLogon», оценки достоинств и недостатков данного ПО.

Литература

1. Ананченко И.В., Смирнов П.И., Шапаренко Ю.М. Аппаратные ключи eToken. Средство защиты eToken Network Logon. – СПб.: изд. РГГМУ, 2015. – 27 с.

2. Ананченко И.В., Шапаренко Ю.М. Использование микропроцессорных смарт-карт для авторизации пользователей в операционных системах. Информационные технологии и системы: управление, экономика, транспорт, право. 2019. № 2 (34). С. 149-153.

Приложение

Образец титульного листа отчета по лабораторным исследованиям

Министерство науки и высшего образования и Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
“Российский государственный гидрометеорологический университет”
Кафедра информационных технологий и систем безопасности

Отчет
по лабораторной работе №__

_____

Наименование лабораторной работы

Дисциплина «Технические средства обеспечения информационной безопасности»

Выполнил:

_____

ФИО студента, номер группы)

Проверил:

_____

(ФИО преподавателя, уч. степень, уч. звание)

Санкт-Петербург

20___ г.

Содержание

Учебное издание

Ананченко Игорь Викторович, канд. техн. наук, доцент
Алейникова Оксана Вячеславовна
Шапаренко Юрий Михайлович, канд. техн. наук, доцент

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ
Часть 2. АППАРАТНЫЕ USB-ТОКЕНЫ И СМАРТ-КАРТЫ JaCarta.
СРЕДСТВО ЗАЩИТЫ JaCarta SecurLogon

Печатается в авторской редакции .

Подписано в печать 23.09.2020. Формат 60×90 1/16.

Гарнитура Times New Roman. Печать цифровая.

Усл. печ. л. 1,75. Тираж 30 экз. Заказ № 974.

РГГМУ, 192007, Санкт-Петербург, Воронежская, 79.