Учебный кейс-стади: Руководство по установке и настройке E-Mail клиента theBat для шифрования почты.

1. Установка, создание почтового ящика.

Скачиваем необходимый дистрибутив TheBat (Найти в Интернете или приобрести у разработчика)

Запускаем на исполнение установщик thebat

Следуем пошаговым инструкциям:

Windows Installer	
Preparing to install	
	Cancel

🚏 The Bat! v4.0.18 Русская Версия - InstallShield Wizard 🛛 🗙
Лицензионное соглашение
соглашение.
Лицензионное соглашение
Данное лицензионное соглашение является соглашением между вами - Пользователем (физическое или юридическое лицо) и компанией Ritlabs SRL (Правообладатель) по использованию программного обеспечения (Программа), принадлежащего компании Ritlabs SRL и сопровождающего данное Лицензионное соглашение.
 Я принимаю условия лицензионного соглашения Я не принимаю условия лицензионного соглашения
InstallShield
< Назад Далее > Отмена

Ждем, пока скопируются файлы:

👘 The Bat! י	v4.0.18 Русская Версия - 1	InstallShield Wizard		_ 🗆 🗡
Установк Устанав.	ка The Bat! v4.0.18 Русска ливаются выбранные компон	я Версия ненты программы.		4
1	Дождитесь окончания уста может занять несколько ми	ановки The Bat! v4.0.18 инут.	Русская Версия. Это	
	Состояние:			
InstallShield –				
		< <u>Н</u> азад Д	алее > От	1ена

Отменяем установку Яндек-бар (если таковая имеется в дистрибутиве):

	Установка компонентов Яндекса
S ndex	Выберите компоненты, которые вы хотите установить:
/	🔲 Персональный поиск Яндекса для TheBat!
	Яндекс.Бар - поиск и другие сервисы Яндекса в вашем браузере
	Также вы можете:
	🔲 сделать Яндекс стартовой страницей
Пожалуйста, прочтит <u>Яндекс.Бара</u> . Продол	е лицензионные соглашения для <u>Персонального поиска</u> и жая установку выбранных компонентов, вы принимаете их условия.
	<u> </u>

При желании можем защитить паролем файлы почтового ящика, которые будут храниться на винчестере. В данном примере для простоты отказываемся от этого, нажимая далее:

попользовать шифрование для почт При использовании этой опции никакая н цанные перед записью будут зашифров корости. Никакие другие пользователи	ным озыки адресных клия информация не будет храниться в открытом виде на вашем диске. Все аны. Метод залиси прозрачен и не приносит заметного падения (включая сетевых) не смогут прочитать ваши данные.
Эднажды выбрав, вы не сможете помен ыбора другого режима сделайте резер оосстановите данные из вашей резервни	ить в течении работы с програмной настройки защиты данных. Для ниую копию, удалите The Batl и установите заново, после чего й копии.
Јифрование (OTFE) доступно только в	The Bat! Professional Edition
Защищать зашифрованные данные	
Fé III	
Haponem Aladdin eToken LISB Token	
Tiaponem C Aladdin eToken USB Token C Rainbow Key1000 USB Token	
Tiaponem Aladdin eToken USB Token Rainbow iKey1000 USB Token	
C Aladdin eToken USB Token C Rainbow iKey1000 USB Token	
Tiaponen Tiaponen Aladdin eToken USB Token Reinbow iKey1000 USB Token	
C Naponevi C Aladdin eToken USB Token C Reinbow (Key1000 USB Token	
Chaponen Construction Aladdin Folken USB Token Rainbow Key1000 USB Token	

ВЫОИРАЕМ МЕСТО НА ЖЕСТКОМ ДИСКЕ, ГДЕ ОУДУТ ХРАНИТЬСЯ ФАЛЫ ПИСЕМ, УКАЗЫВАЕМ КАКИЕ СОЗДАВАТЬ ЯРЛЫКИ	Выбираем место на жестком диске,	где будут храниться фалы писем.	указываем какие создавать ярлыки:
---	----------------------------------	---------------------------------	-----------------------------------

🔀 Первый запуск The Bat!	? ×
Г Основной почтовый каталог The Bat! (для хранения почты)	
О Папка данных текущего пользователя	
О Общая папка данных пользователей компьютера	
О Подпапка "MAIL" папки программ (для всех пользователей)	
Определяемый пользователем каталог	
D:\mail	Изменить
г Группа Главного меню (под кнопкой Пуск)	
Programs	Изменить
 Создать ярлык на <u>Р</u>абочем столе ✓ Создать ярлык в <u>Г</u>лавном меню (под кнопкой Пуск) ✓ <u>Д</u>обавить The Bat! в меню "Отправить" 	
< <u>Н</u> азад	ОК Отмена

Далее происходит процедура создания нового почтового ящика в программе:

ящик (установка "с нуля"), либо восстановить данные из ранее сделанной резервной копии.
Создать новый почтовый ящик
С <u>В</u> осстановить данные из резервной копии

Название ящика и путь к нему:

Введите что это н уже нахо этих фай для посл	название ящика и выберите для не название не используется другим яш одятся файлы конфигурации почтов пов будут использованы в качестви едующих шагов.	го каталог. Убедитесь, циком. Если в каталоге юго ящика, данные из е значений по умолчаник
<u>Н</u> азвание	ящика:	
Личный я	ащик 1	
Домашний	й каталог:	
Домашни <по умол	й каталог: 1чанию>	
Домашниі <по умол	й каталог: ічанию> <u>О</u> бзор	По умолчанию
Домашниі <по умол	й каталог: ічанию> Обзор	По умолчанию
Домашниі <по умол	й каталог: тчанию> 	По умолчанию
Домашниі <по умол	й каталог: тчанию> 0бзор	о умолчанию

Дальнейшая конфигурация:

	Введите данные e-mail. Эта информация будет использоваться по умолчанию в ваших письмах для формирования данных об отправителе.
	Выше полное имя (например, Иван Петров):
	Личный ящик 1
	Appec e-mail:
	test@test.ru
	Организация:
E	Дом
1 3 1	

Выбор и настройка почтовых протоколов, по которым производится обмен данными с сервером. Данный момент настройки специфичен для каждого отдельно взятого почтового сервиса. Необходимые настройки можно узнать у Вашего поставщика почтовых услуг:

Для доступа к серверу использовать протокол • РОРЗ - Post Office Protocol v3 • IMAP4 - Internet Message Access Protocol v4 • MAPI - Microsoft Exchange Server • МАРІ - Microsoft Exchange Server • Сервер для получения почты (например, mail.domain.tld): pop3.gmail.com Aдрес сервера ≦МТР (например, smtp.domain.tld): smtp.gmail.com Moй сервер SMTP требует аутентификации	Введите адреса почтовых серверов. Эти адреса Вам предоставляет Ваш системный администратор или провайдер Интернета. SMTP-сервер используется для отправки писем, POP3-сервер используется для получения писем.
 POP3 - Post Office Protocol v3 IMAP4 - Internet Message Access Protocol v4 MAPI - Microsoft Exchange Server Сервер для получения почты (например, mail.domain.tld): pop3.gmail.com Адрес сервера SMTP (например, smtp.domain.tld): smtp.gmail.com Moй сервер SMTP требует аутентификации 	Для доступа к серверу использовать протокол
 МАР4 - Internet Message Access Protocol v4 МАРІ - Microsoft Exchange Server Сервер для получения почты (например, mail.domain.tld): рор3.gmail.com Адрес сервера ≦МТР (например, smtp.domain.tld): [smtp.gmail.com ✓ Мой сервер SMTP требует аутентификации 	POP3 - Post Office Protocol v3
Сервер для получения почты (например, mail.domain.tld): pop3.gmail.com Адрес сервера <u>S</u> MTP (например, smtp.domain.tld): smtp.gmail.com ✓ Мой сервер SMTP требует аутентификации	C MAPI - Internet Message Access Protocol v4
pop3.gmail.com Адрес сервера <u>S</u> MTP (например, smtp.domain.tld): smtp.gmail.com Г Мой сервер SMTP требует аутентификации	Сервер для получения почты (например, mail.domain.tld):
Адрес сервера <u>S</u> MTP (например, smtp.domain.tld): [smtp.gmail.com Г Мой сервер SMTP требует аутентификации	pop3.gmail.com
smtp.gmail.com Мой сервер SMTP требует аутентификации	 Адрес сервера SMTP (например, smtp.domain.tld):
🖉 Мой сервер SMTP требует аутентификации	smtp.gmail.com
	🔽 Мой сервер SMTP требует аутентификации

Настройка параметров аутентификации для почтового ящика:

Укажите данные метод АРОР, убед Если поле пароля попытки получит	учётной записи на сервере РОРЗ. Если выбран цитесь, что этот метод поддерживается на сервере. оставить пустым, пароль будет запрошен во время ь доступ к серверу.
Пользователь: Пароль:	test
☑ Оставлять пис ☑ Использовать	ьма на сервере шифрованный метод аутентификации (АРОР)

	Укажите способ подключения к Интернет. Убедитесь что проток TCP/IP установлен и правильно настроен на Вашей машине.								
	• • Через докальную сеть или с	соединение вручную							
100	С Через <u>Удаленный доступ:</u> <u>П Р</u> азрывать связы по око	ВуFly							
	< Назад	Далее > Отмена							

Выбор соединения, через которое будет производиться подключение к серверу:

Окно приглашения просмотра детальных настроек почтового ящика:

	Первоначальная настройка почтового ящика завершена. Вы можете проверить остальные свойства почтового ящика, такие как шаблоны, управление письмами, прямо сейчас или сделать это позже. Нажмите кнопку "Готово", чтобы добавить этот почтовый ящик в список.
	Хотите проверить остальные свойства почтового ящика? С Нет С Да
-	< Назад Сотово Отмена

В окне свойств почтового ящика можно произвести детальную настройку самых различных параметров для данного

	ящика:	
🔀 Свойства почтового ящика -	- Личный ящик 1	×
Общие сведения Транспорт Управление почтой Параметры Файлы и каталоги Шаблоны Новое письмо Ответ Пересылка Подтверждение прочт Сохранение в файл Файлы Факлочение Заметки Чат	Название: Личный ящик 1 Сертификаты Визитная карточка Информация для поля От	
	ОК Отмена Справка	

Наиболее важной частью является настройка транспортных параметров. Тут указываются конкретные версии протоколов и порты доступа для получения и отправки почтовых сообщений:

🧮 Свойства почтового ящика -	Личный ящик 1
Общие сведения Транспорт Управление почтой Параметры Файлы и каталоги Файлы и каталоги Новое письмо Ответ Пересылка	Отправка почты <u>S</u> MTP-сервер: smtp.gmail.com Аутентификация Соединение: Безопасное на станд. порт (STARTTL Порт: 587 Получение почты Поут. сервер: pop3.gmail.com Аутентификация
Годтверждение прочт Сохранение в файл Девизы Звук Подключение Заметки Чат	Пользователь: test Протокол: РОРЗ Пароль: ●●●●●●●●●● Соединение: Безопасное на спец. порт (TLS) ■ Порт: 995
	<u>Т</u> аймаут сервера: 60 ♀ сек. <u>Т</u> ип доставки: Немедленная ▼ Совмещенная доставка (получение + отправка)
4 •	ОК Отмена Справка

Для удобства создадим на рабочем столе ярлык на файл The bat: Переименуем его в «The Bat». В итоге на рабочем столе будет иметься ярлык:



Запускаем программу, используя этот ярлык, и переходим к процедуре регистрации:

Для этого выбираем в меню «?» пункт «Регистрация»:

🚳 The Bat!					
<u>П</u> исьмо <u>С</u> пециальное П <u>а</u> пка <u>Я</u> щик	<u>И</u> нструменты	<u>В</u> ид Св <u>о</u> йства	?		
Название	Непрочитано	Bcero		<u>Р</u> азделы	3
🕀 🛅 Личный ящик 1		1		<u>С</u> овет дня	
🐼 Входящие		1		WWW страница Неофициального FAQ (ЧаВо)	-fhu
- 💽 Исходящие		0	-	Как зарегистрироваться?	- 10
Справленные		U		Регистрация	
Входящие - Известные ад		0		- OTICI POLIN	1
		_		Письмо авторам	•
				О <u>ф</u> ициальная WWW страница программы	
				Проверить <u>н</u> аличие обновлений	
				<u>О</u> программе Alt+F1	
			Т		

Отображается окно для ввода лицензионного ключа:

🙆 The Bat!					<u>_ ×</u>
Письмо Специальное Папка Ящи	к <u>И</u> нструменты <u>В</u> ид Св <u>о</u> йства	7			
Название	Непрочитано Всего	🛛	s. a II		·
🗗 🛅 Личный ящик 1	1				
	1			у Поиск:	
Паравленные	ŏ	🖂 🖸 📙 От	Кому	Тема	🖓 Получено
🦾 🕑 Входящие - Известн 💓 🗖	ожалуйста, введите регистрац	ионный ключ	- · ·	X	9:54
		OK	Отмена	Справка	<u> </u>
		I CMG. THE BALL			
		Welcome to The Bat! Once you have installed	d The Bat!, you r	eceive at your di	sposal not
К • • H Все Непрочитано /	Адреса	just an ordinary email facilitate your routin your correspondence. I requirements It will	client. The Bat! e work, lessening t will adjust its become your relie	is something great the time you spect elf to your needs hle assistant he	ater. It will nd daily for and Ining you deal
🔀 Личный ящик 1 😤 Без пароля					



Once you have installed The Bat!, you receive at your dispos-



. .. .

.

2. Настройка использования OpenPGP для шифрования и подписывания почты.

Сначала необходимо сгенерировать ключевую пару. Выбираем в меню: Инструменты\OpenPGP\Управление ключами:

😽 The Bat!						
Письмо <u>С</u> пециальное П <u>а</u> пка <u>Я</u> щи	к Инструменты Вид Свойства ?					
Название Непроч В-С Gmail С Входящие С Исходящие С Отправленные	ни 🥵 Адресная книга 🔍 Поидк 🕞 SmartBat 🚯 Пданировщик 4	F8 F7 S S S S S F6 F6 F6 F6 F6 F6 F6 It+F11 Поиск:				
Корзина	почтовыи цат ⊇кспортировать письма Импортировать письма	Кому Тема ФП_ Jemy Connection Aleh Karatkevich Интерактивные технолог 24 ок monov V.A. 4mamont@gmail Fwd: "Приборостроение "2 24 ок addy.com 4mamont@gmail Save 15% now through Su 23 ок				
	<u>Р</u> езервная копия Восстановить из резервной <u>к</u> опии Си <u>н</u> хронизировать Криптография и <u>б</u> езопасность	нные _ С флажком ction <webmaster@cisco.netacad.net> I <4mamont@gmail.com> ▶ э технологические вебинары Cisco</webmaster@cisco.netacad.net>				
	ОрепРGР Олучить почту (все ящики) Отправить почту (все ящики)	Выбор версии OpenPGP Аlt+F2 Управление ключами OpenPGP Настройка OpenPGP мероприя тиях !				
и • • • Все Непрочитано /	Monyчить и отправить почту (все ящики) Webinars.rtf ~53 K6	F11 оду им хотим представить вашему вниманию серию интерактивных технологических вебинаров Cisco. Ссе вебинары серии проводятся на русском языке инженерами Cisco из стран СНГ и позволяют продемонстрировать возможности современных технологий, используя ресурсы набораторий Cisco. Вебинары будут проводиться с помощью ↓ ► ► HTML Webinars.rtf				

Запускается мастер создания ключей:

😂 Управле	ение ключами ОлелРБР	
Правка Кл	🧮 Мастер создания ключей OpenPGP	×
Ключи ⊞• ©⊳ <i>Ritla</i>t	Для того, чтобы Вам могли посылать шифрованные письма, Вы должны создать пару ключей.	ие ий Открытый
	Ваш ключ также может быть использован для подписи электронных документов.	
	Пара ключей состоит из "открытого ключа" и "личного ключа". Открытый ключ должен быть доступен всем, личный ключ должен храниться только у Вас.	
	Если Вам нужна информация о том, что такое пара ключей и как это работает, нажмите кнопку "Справка".	
	Нажмите "Далее" для продолжения.	
	< <u>Н</u> азад	

Проходим предлагаемые шаги. Выбираем какому адресу должна соответствовать ключевая пара:

🗮 Мастер создания ключей OpenPGP	×
Какие ФИО и e-mail адрес должны соответствовать этой паре ключей?	
Указывая ФИО и e-mail адрес, Вы сообщаете своим корреспондентам, что ключ, который они используют, принадлежит Вам.	
E-mail adpec:	
4mamont@gmail.com	
	_
< <u>Н</u> азад <u>Далее</u> > О <u>т</u> мена <u>С</u> правка	

Выбираем длину ключа и его срок действия:

🐱 Мастер создания ключей OpenPGP	×	Macтep создания ключей OpenPGP	×
Укажите размер ключа. Как правило, ключи большего размера более надежны, но и более медленны. Для большинства применений вполне достаточно 1024 бит. Ключи размером более 1024 или 2048 бит могут не быть восприняты некоторыми программами. Ключи размером менее 768 бит считаются некотерыми про сегодящиним меркам, их рекомендуется использовать		Вы можете установить дату истечения срока действия Вашего ключа. Когда срок действия ключа истечет, Вы больше не сможете его использовать для шифрования или создания подписи. Тем не менее, им можно будет расшифоревать письма и проверать подпись.	
Размер ключа ○ 768 ○ 1024 ○ 1536 ○ 2048 ○ По выбору (384-4096 бит):		После того, как вы создадите ключ, Вы уже не сможете изменить дату истечения срока действия ключа. Дата истечения Срок истекает: 25 октября 2010 г. Без ограничения срока	
< <u>Н</u> азад Далее > О <u>т</u> мена <u>С</u> правка		< <u>Н</u> азад Далее > Отмена <u>С</u> правка	

Защищаем файл ключей паролем. Пароль необходимо помнить и не терять, так как его нужно будет использовать всякий раз при подписывании\зашифровке писем. Завершаем создание ключевой информации.

Теперь пару ключей можно видеть в списке ключей:

😂 Управление ключами OpenPGP					<u>_ ×</u>
Правка Ключи					
Ключи	Дейс	Дов	Размер	Описание	
Proven Proven Proven Proven Proven MamONt <4mamont@gmail.com> Proven MamONt <4mamont@gmail.com> MamONt <4mamont@gmail.com> Proven MamONt <4mamont@gmail.com> Prove	• •		2048 1024	Описание Истекший Открытый ключ RSA Пара ключей RSA ОрепPGP ID пользователя Экспортируемая подпись OpenPGP	
<u></u>					

Для ведения защищенной переписки пользователи должны сгенерировать ключевые пары и обменяться своими открытыми ключами.

Экспорт открытого ключа производится следующим образом:

👺 Управление ключами Оре	nPGP					
Правка <u>К</u> лючи						
Ключи		Дейс	Дов	Размер	Описание	
🕀 💷 Ritlabs Corporate Key (offic	ce@nitlabs.co	-	<u> 77777</u>	2048	3 Истекший Открытый ключ RSA	
🕀 🚼 MamONt < 4mamont@gr	nail.com		V7777	1024	Пара ключей RSA	
🖻 🙀 Mam0Nt <4mamont@	<u>К</u> опировать				OpenPGP ID пользователя	
🦾 🔏 Mam0Nt < 4mamor	Вст <u>а</u> вить				Экспортируемая подпись OpenPGP	
	<u>У</u> далить					
	Подписать					
	Boopouurt					
	Саррешите					
	запретить					
	Добавить имя					
	Аннулировать					
	Установить по у	мопчанин	n			
-	s aTausaura us A	nevr serim				
	<u>И</u> мпорт					
	⊇кспорт					
	Сво <u>й</u> ства ключа					
-						

кспортироватн	открытые кл	ючи OpenPGP в файл			<u>?</u> ×
Save jn:	Contemp		•	G 🖸 🖻 🖽	
Mu Bacant					
Documents					
Desktop					
My Documents					
My Computer					
	Claure and	-			Cours
My Network Places	rile <u>ri</u> ame:	открытый ключ.кеу			Jave
	Save as <u>t</u> ype:	Все файлы (*.*)		<u> </u>	Cancel

Выбираем путь, куда сохранить открытый ключ и даем имя фалу:

На вопрос об экспорте секретного ключа отвечаем «Нет»:

😽 Управление ключами OpenPGP		- 🗆 ×
<u>П</u> равка <u>К</u> лючи		
Ключи	Дейс Дов Размер Описание	
🕀 💽 Ritlahs Corporate Key Coffice@ritlahs.co	🔶 🚾 2048 Истекший Открытый ключ RSA	
🖻 🔚 MamONt <4mamont@gmail.com>	🔶 🚾 1024 Пара ключей RSA	
🗗 🙀 MamONt <4mamont@gmail.com>	🥮 OpenPGP ID пользователя	
🎂 🏀 Mam0Nt <4mamont@gmail.com>	Экспортируемая подпись OpenPGP	
	Управление ключами OpenPGP Экспортировать также и личные ключи OpenPGP? <u>Yes No</u>	

Полученный файл необходимо отправить в чистом виде тому адресату, которому вы потом планируете слать подписанные и зашифрованные письма.

Тот адресат в свою очередь <u>должен прислать вам свой открытый ключ</u>, который вы должны импортировать в систему:

🔐 Упра	вление ключами OpenPGP		
Правка	<u>К</u> лючи		
Ключи	Подписать	Ctrl+S	Дейс Довери
🕀 🖘 A	Установить по умолчанию	Alt+D	
<u>Ө</u> ЗМ	<u>Д</u> обавить имя	Alt+A	- 🔶 🖂
📄 🕀	Создать новую пару ключей	Ctrl+N	
	<u>Р</u> азрешить	Ctrl+E	
	<u>З</u> апретить	Ctrl+D	
	Аннулировать	Ctrl+R	
	Импорт	F2	
	<u>Э</u> кспорт	F3	
	Сво <u>й</u> ства ключа	Enter	
I '			a

После обмена ключевой информацией можно приступать к ведению защищенной переписки. При создании письма перед его отправкой нужно в меню «Криптография и безопасность» указать использование «Авто - OpenPGP» и установить оба переключателя: «Зашифровать перед отправкой» и «Подписать перед отправкой». Внизу такого письма мы увидим соответствующие значки:

I



Перед отправкой такого письма будет запрошен пароль для доступа к секретной ключевой информации:

<mark>malli</mark> 😹 Введите пароль Ор	enPGP		×		
Введите пароль OpenPGP для М <i>конфиденциально</i> @gmail.com>					
			Caracana		
		Отмена	Справка		

Получив зашифрованное и подписанное письмо вы будете уведомлены об этом системой:

襘 Просмотр па	апки Входящие ящика Gmail	<u> </u>
Письмо <u>С</u> пециа	альное Переход Криптография и безопасность Вид	
🖢 • 🥗	Поиск: 🚺 🖄 😒 🥪 🕞 🔛 Тоиск: Г	
От: Кому: / Тема:	MamONt <4mamont@gmail.com> 4mamont@gmail.com Тестовое зашифрованное письмо.	
Часть.txt 129 байт	Это письмо зашифровано в формате PGP. Для того, чтобы его расшифровать, нажмите кнопку криптосистемы на панели заголовка. нажать для расшифровки	

Для расшифровки нужно нажать соответствующую кнопку, находящуюся в заголовке письма.

После запроса пароля и расшифровки открывается доступ к расшифрованной информации:



А в журнале регистрации проверок подписей отображается запись об успешной проверке подписи:

🕼 История проверок цифровой подписи OpenPGP				
Время	Подписал	Действит.	Время (UTC)	
25.10.2009 8:22:24	Mam0Nt <4mamont@gmail.com>	Действит.	25.10.2009 8:20:28	

Важное в заключение:

1. Не следует делиться ни с кем своей закрытой ключевой информацией.