novateca

Information protecting in cyberspace: theory and practice

integrator.md

Кибернетическая безопасность: это совокупность технологий, процессов и различных видов деятельности, направленных на защиту информационно-вычислительных сетей, компьютеров и программного обеспечения от атак, повреждений и несанкционированного доступа

(NATO Communications and Information Agency Definition)

Информационная безопасность: обеспечение конфиденциальности, целостности и доступности информации, а также таких ее свойств как достоверность, подлинность, неотказуемость и надежность

(ISO/IEC 27001:2005 Information security management system Definition)

Защита информации:

Топ 5 задекларированных финансовых потерь:

1. Sony - $171 mln
2. Citigroup - $2.7 mln
3. Stratfor - $2 mln
4. AT&T - $2 mln
5. Fidelity Investments - $1 mln

Wild World Web: почему это актуально?

Статистика распространения уязвимостей на сетевом периметре

79%	Словарные пароли пользователей
63%	Внедрение операторов SQL
58%	Интерфейсы управления оборудованием доступны любому пользователю сети Интернет
53%	Межсайтовое выполнение сценариев
47%	Хранение важных данных в открытом виде
47%	Раскрытие конфигурационной информации в веб-приложениях
47%	Недостаточная защита от подбора учетных данных
47%	Использование открытых протоколов передачи данных
42%	Выход за пределы каталога (Path Traversal)
32%	Раскрытие информации об идентификаторах

Вывод: в каждом третьем случае любой внешний злоумышленник может получить полный контроль над всей инфраструктурой

Wild World Web: почему это актуально?

Наиболее распространенные уязвимости во внутренней сети

Выводы:

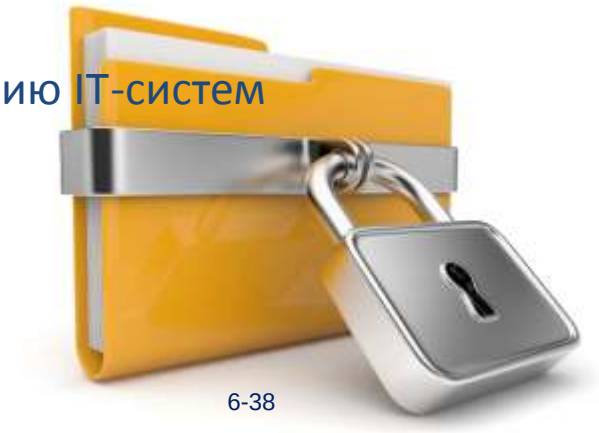
- внутренний непривилегированный злоумышленник в 84% случаев может получить максимальные привилегии в критически важных системах;

- в среднем каждый пятый пользователь переходил по фишинговым ссылкам и осуществлял ввод учетных данных либо запуск предложенных файлов

Защита информации: текущая ситуация

Threat Track Security Inc. отчет:

- 55% организаций обеспечили дополнительное обучение по вопросам ИБ для своих сотрудников;
- 52% организаций пересмотрели уровень доступа к информации для своих сотрудников;
- 47% компаний стали уделять больше внимания нестандартному поведению сотрудников в Сети;
- 41% компаний ввели более жесткие требования при найме новых сотрудников;
- 39% компаний сократили права по администрированию IT-систем своим сотрудникам



Источник информации: www.securitylab.ru/news/449409.php

Password protection: new way to play an old song

novateca

Общие рекомендации к сложности паролей

- **длина**: не менее 8 символов;
- **повторяемость**: 5 последних;
- **сложность**: буквы, цифры, спецсимволы;
- **срок действия**: до 90 дней

Результаты исследований

8 символов: N^a&$1nG был бы взломан за 3,75 суток

28 символов: GoodLuckGuessingThisPassword был бы взломан за 17,74 лет

атака по словарю: из 626718 паролей 54% взломаны в течении минут

Источник информации:
http://www.allcio.ru/safety/65529.html

Анализ результатов исследований

1. Пароли, по-прежнему уязвимы
2. Ужесточение требований к паролям приведёт к «обратному эффекту»:

   - использование единого пароля для всех приложений;

   - периодические «забывания» паролей;

   - выбор простых паролей, подходящих к требованиям;

   - записывание паролей;

Варианты решений

1. **Общие или чувствительные ИС**: «Маскировка деревьев в лесу»

2. **Жизненно важные ИС**: двухфакторная (многоэтапная) аутентификация:
   - двухфакторная аутентификация (smart-карты);
   - многоэтапная аутентификация (sms уведомления)

3. **Критические ИС**: программно-аппаратные средства:
   - разовых паролей (One Time Password устройства);
   - генерирование паролей

The weakest link in security

Why use social engineering?

1. Because it works!

Always has…

Always will...

To: You
Subject: Assistance required
We are top official of the Federal Government contract review panel who are interested in imporation of goods into our country with funds which are presently trapped in Nigeria. In order to commence this business we solicit your assistance to enable us transfer into your account the said trapped funds.

2. Great return on investment

Hacker To-Do List

- Footprint network
- Scan (don't get caught)
- Enumerate systems
- Find unpatched vulnerability
- Develop malware or
- Brute force password
- Look for interesting tidbits

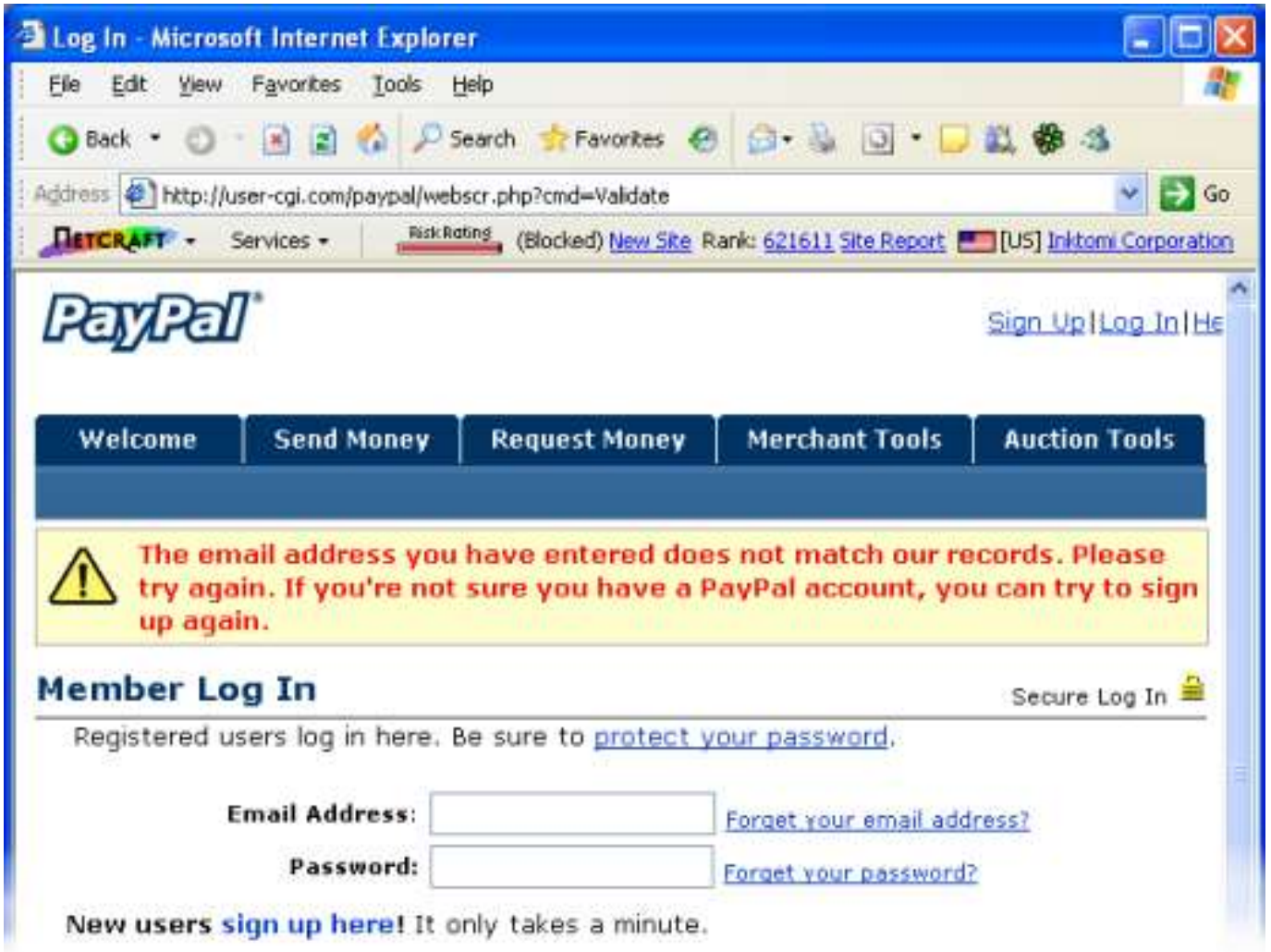
Vs.

Hacker (revised) To-Do List

- Do web search on target company, find phone list
- Call random employee
- Pretend to be help desk testing new web portal
- Have helpful employee test portal by entering credentials

Why use social engineering?

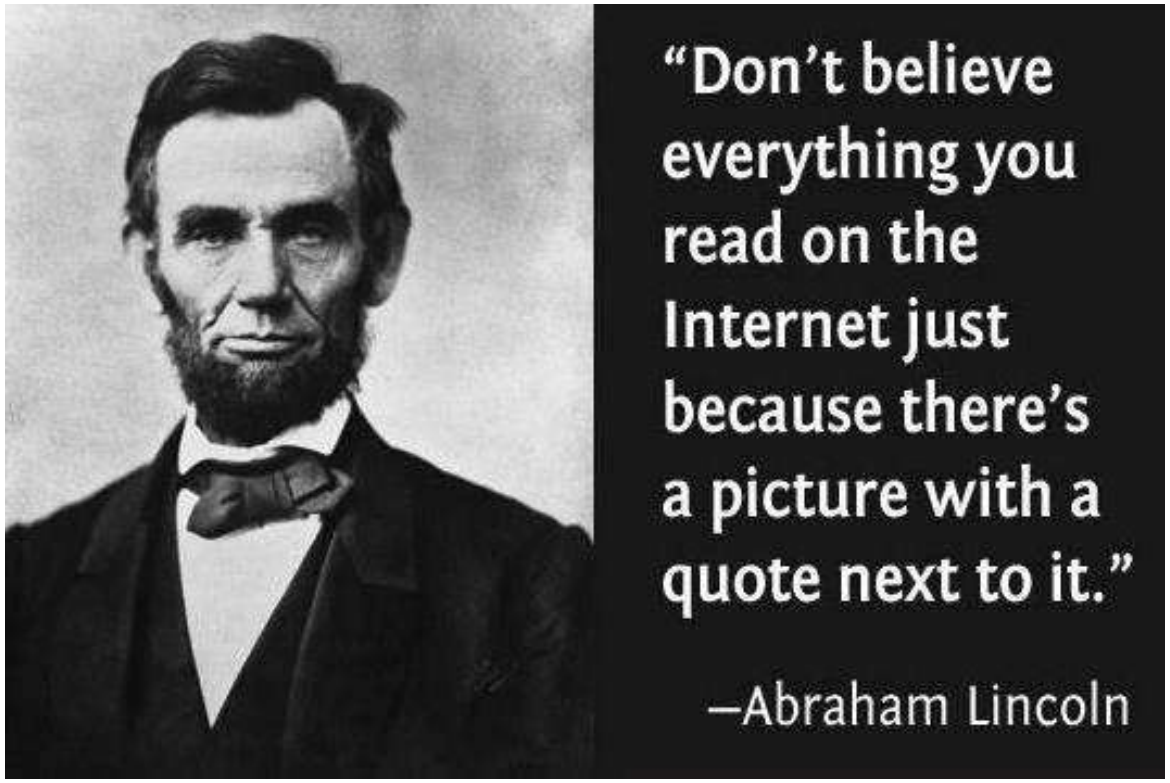
3. It is effective



Why does it work?

novateca

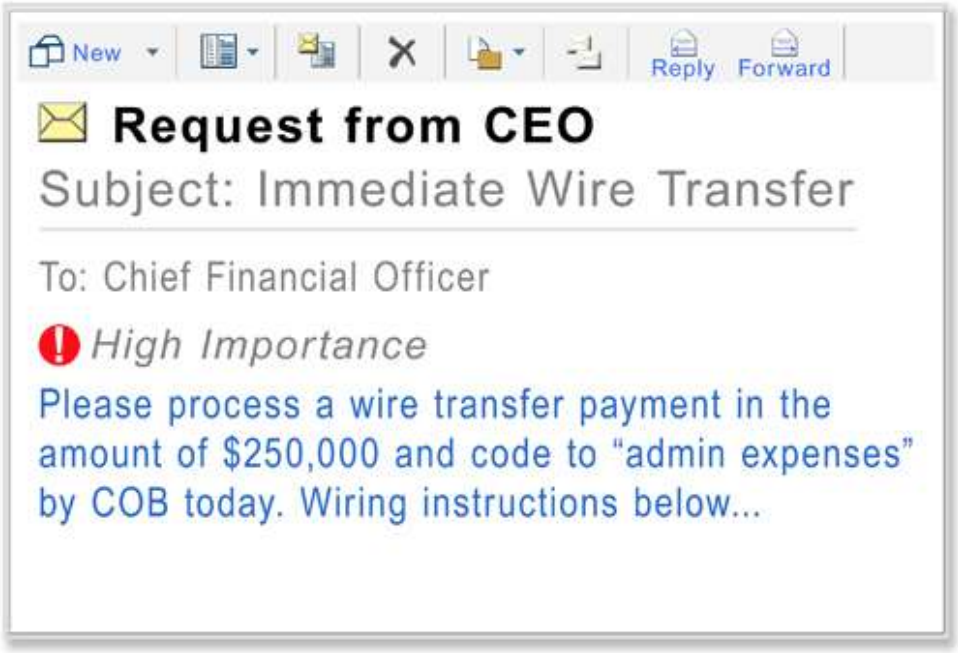
1. Trust



Most people believe that no one is out to do them harm

novateca

2. Urgency/Scarcity



Business Email Compromise has resulted in approximately $750 million in losses across more than 7,000 US companies from October 2013 – August 2015

Source: fbi.gov

Everything is a priority and what we need is in short supply

3. People assume innocent mistakes

If information doesn’t fit the situation then they ignore it

novateca

4. People are helpful, especially to strangers

An organization’s drive for customer service amplifies this tendency and often leads to employees providing more information than they need to

novateca

5. Curiosity

People are curious by nature and it often outweighs caution and even common sense.

novateca

5. We love to reciprocate

If someone is nice to you then you are often nice to them

5. The power of authority

People defer to those in (or who appear to be) in position of authority or power.

Tools of the trade

- **Elicitation**: Extract information out of what appears to be an innocent conversation

- **Pretexting**: The act of creating an invented scenario or backstory to persuade a target to provide information or perform some action

- **Watering hole attack**: Determine websites that your target visits frequently that are less secure than the target's organic information assets

- **Low tech works as well**

- **Information collection**

HELP WANTED
Requirements
Deep knowledge and experience troubleshooting the following technologies:
Windows 2012 Server, Microsoft SQL Server, VMWare, Active Directory, DNS, DHCP, Lync, Exchange Server and WINS.
Understanding of PowerShell to drive efficiencies through automation of repeatable processes.
Strong Analytical and Team Player Skills.
Strong Customer Service Skills.
Seven years Windows PC and Server support experience.

1. Awareness training:

- Be purposeful in who gets what training and how often
- Emphasize critical thinking
- Think about a human patch cycle – make people aware of new scams
- Does need to be a balance with customer service

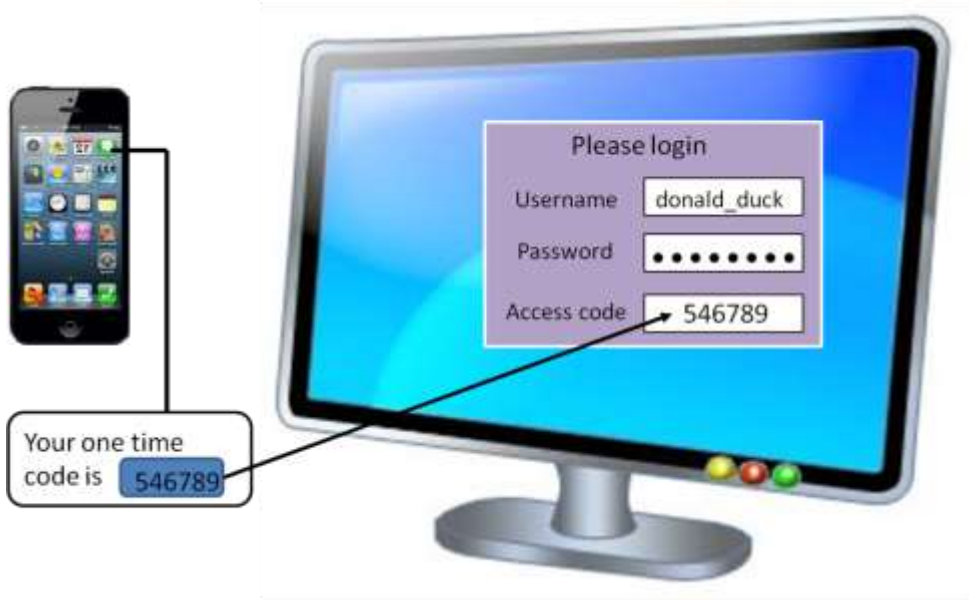
2. Protect critical information:

- Public internet, social media postings
- Photos of building access badges, name tags, org charts
- Remote user instructions for VPNs, portals, and yes - even passwords
- Take into consideration spelt or sounding domain names, add rules to IDS to look for these

novateca

3. Make it harder to use information that is gathered

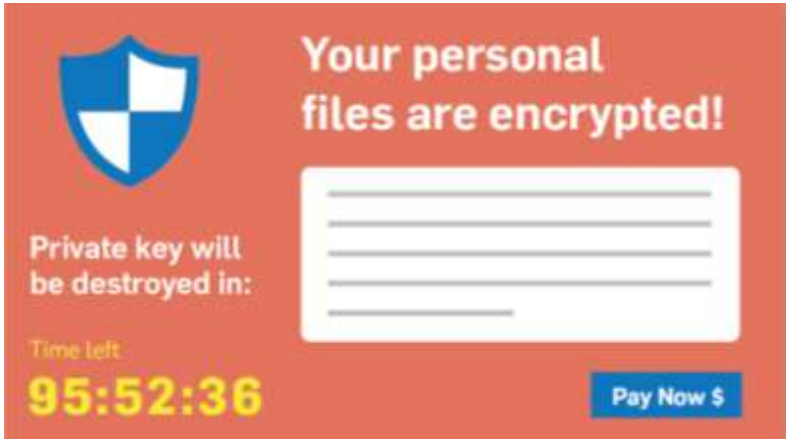
- Two factor authentication
- Network segmentation
- Use time of day or location based access controls



Ransomware

Особенности проникновения

- способ проникновение: (электронная почта, съёмные носители)
- используются «ключевые» слова и тематика
- к письму обязательно прикреплено вложение в виде файла с расширениями (.js, .cmd, .bat, .vba, .ps1)
- заражение происходит при открытии приложенного файла
- антивирусные программы не обнаруживают вредоносный файл



novateca

Признаки заражения

Все файлы были ВРЕМЕННО ЗАБЛОКИРОВАНЫ с помощью алгоритма RSA-1024

1. Это инструкция, которая поможет разобраться с Вашей проблемой. Её решить вполне возможно, не переживайте.

2. Для решения данной проблемы нужно объединить наши общие ресурсы.
Ваши ресурсы:
— e-mail и доверие
— электронная валюта «за урок»
Наши ресурсы:
— Возможность разблокировать Ваш ключ (дешифровщик уже у Вас есть — DECODE.exe)
— Предоставим гарантии — после оплаты ключ будет передан, согласно договоренности
— Консультации после оплаты

3. Мы не из тех, кто шифруют данные, получают средства и затем пропадают.
В данном случае Вы и вправду имеете возможность разблокировать файлы.
Только есть небольшое временное ограничение (срок годности ключа не вечный)
Откладывать вопрос «на потом» также не вариант, плюс верить в чудеса не стоит.

4. У Вас есть два варианта:
а) Форматировать диски и вернуть 0% файлов — неразумно
б) Заплатить за свою невнимательность, вернуть все файлы и получить консультации — вполн правильно

5. Итак, попробуйте запустите Ваш дешифратор из архива. Вам напишет, что ключ не найде

Методы противодействия:

- не запускайте всё, что приходит от неизвестных адресатов
- не открывать непонятные вложения, не соответствующие названию или предполагаемому содержанию
- резервное копирование

novateca

Обеспечение безопасности в социальных сетях

integrator.md

novateca

Существующие угрозы:

- дети (психологическое и сексуальное насилие);
- угрозы личной безопасности;
- мошенничество и шантаж;
- помеха в карьере;
- отсутствие анонимности (человек на ладони)

novateca

Советы, обеспечивающие минимальную безопасность:

- меньше конкретики;
- скептицизм - ваш лучший друг;
- думайте, что вы публикуете;
- не теряйте бдительность;
- проверяйте свои параметры конфиденциальности;
- сложные пароли;
- не ведите важные деловых и личные переговоры через сети

Безопасность персональных данных в социальных сетях

Методы защиты:

1. Используйте механизмы безопасности, предоставляемые социальными сетями (доступ к активам, https, smart-phone);

2. Используйте общие механизмы безопасности, не привязанные к социальным сетям (https);

3. Пребывая в социальной сети, совершайте действия, не угрожающие вашим персональным данным.

novateca

What to Do After a Data Breach: a Step-by-Step Guide:

1. Determine what was stolen.

2. Change all affected passwords.

3. Implement and Enforce Policies.

4. Contact Outside Parties

5. The most important step to take after a data breach is.... **To understand the root of the issue**

6. Test the Security Fix

novateca

Общие правила информационной безопасности

Общие рекомендации по использование вычислительной техники :

1. Использовать ПО для защиты от злонамеренного кода, антиспама и антифишинга

2. Не использовать Wi-Fi зоны для проведения банковских операций или on-line покупок.

3. Регулярно устанавливать обновления безопасности из надежных источников

4. Не используйте нелицензионное ПО

MCloud: Platforma Tehnologică Guvernamentală Comună

MCloud: nivele de securitate

- securitatea fizică a centrelor de date şi a echipamentelor de procesare a informaţiei;
- managementul riscurilor de securitate a informaţiei şi continuitatea afacerii
- securitatea infrastructurii de reţea;
- securitatea infrastructurii virtuale;
- controlul accesului şi securitatea datelor;
- securitatea aplicaţiilor software;
- monitorizarea şi testarea securităţii;
- managementul operaţiunilor;

Basic cryptography:

Integrity: applying hashing algorithm against entire message;

Nonrepudiation (Identity of sender): enciphering the message digest using sender private key;

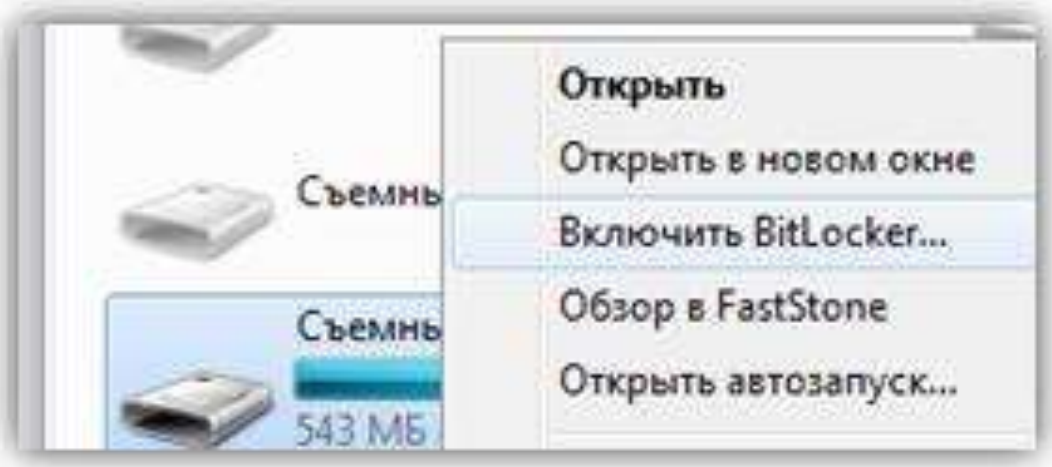
Confidentiality:
- encrypting the message with symmetric key;
- enciphering the symmetric key using receiver public key

Authentication: if the public key deciphers the message satisfactory, one can be sure of the origin of the message because only the sender could have encrypt the message

BitLocker: a disk encryption solution

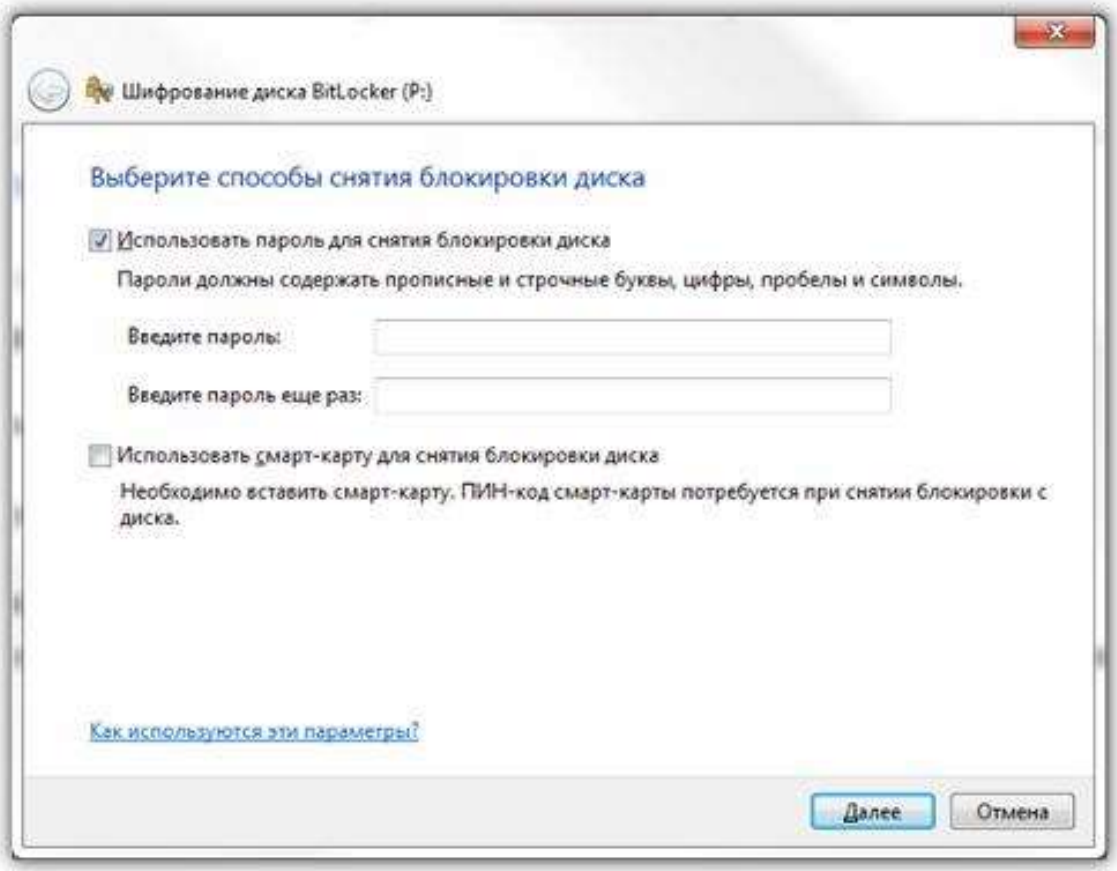
novateca

1. Включение



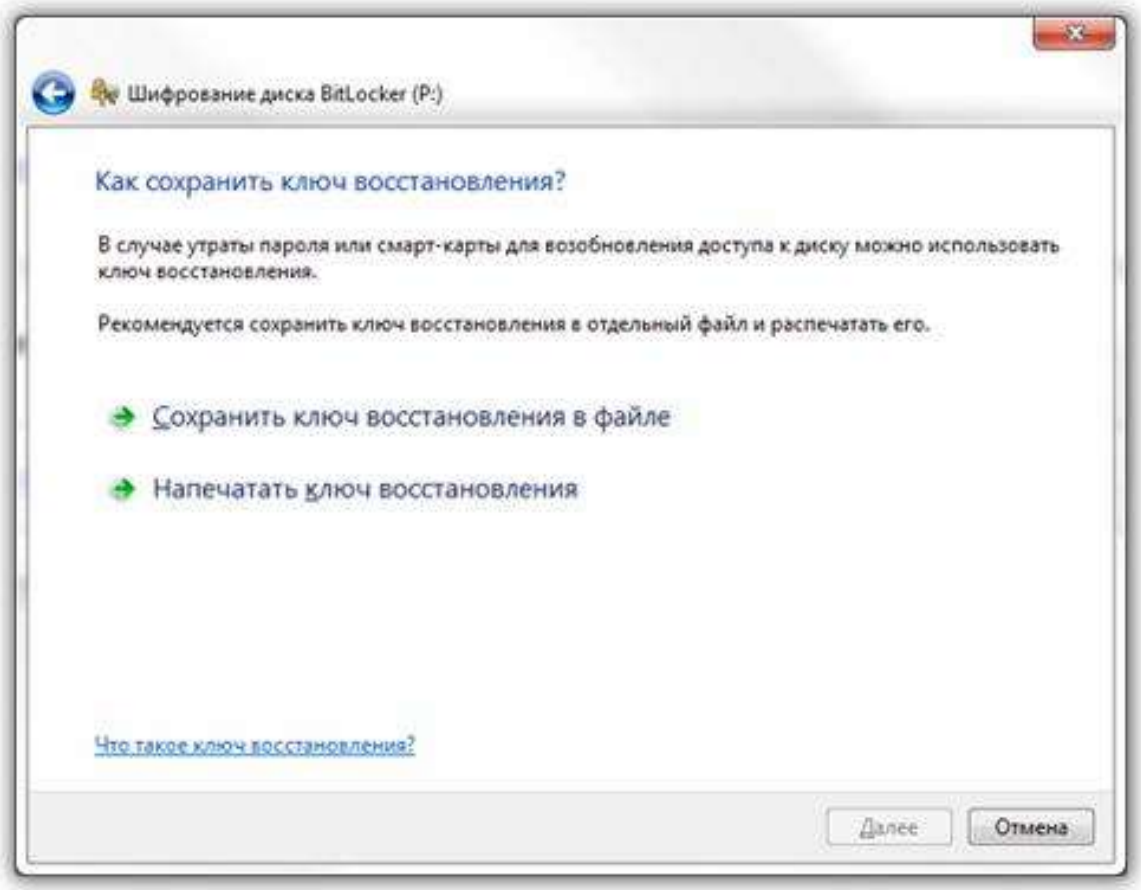
BitLocker: Windows 7 example

2. Пароль для шифрования



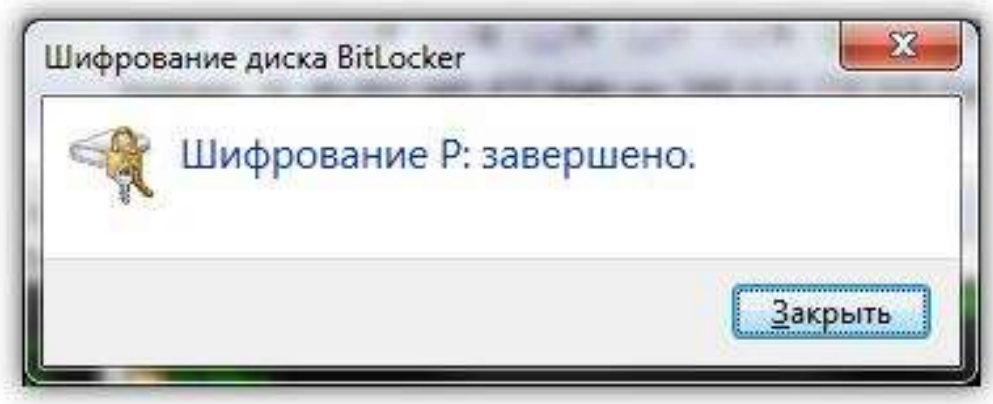
novateca

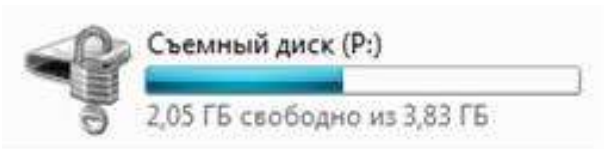
3. Ключ для восстановления



novateca

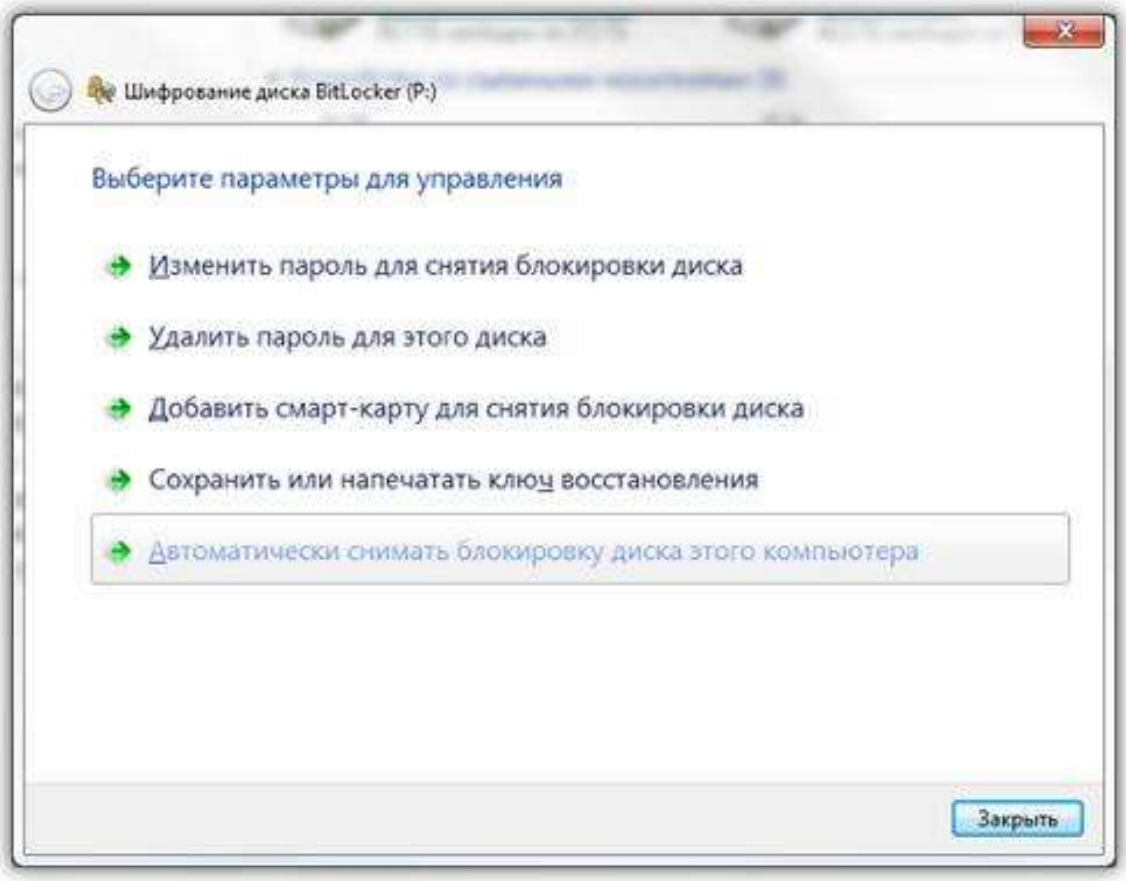
4. Шифрование





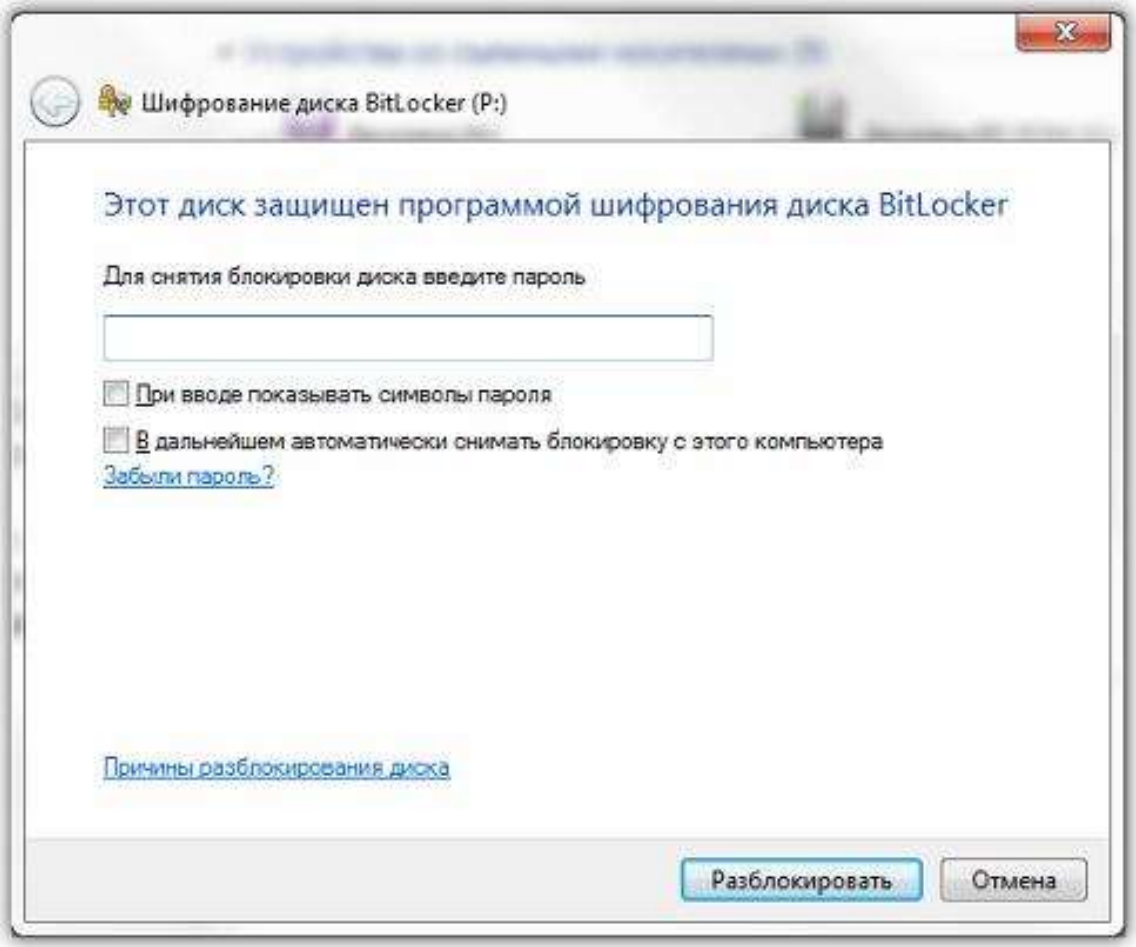
novateca

5. Параметры для управления bitlocker



novateca

6. Использование bitlocker с другими системами




THE END
Thank you for listening!