



Братство организаторов
студенческого самоуправления



ПАМЯТКА ПО ОБЕСПЕЧЕНИЮ
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
УРОВЕНЬ «НОВИЧОК»

Памятка по обеспечению безопасности персональных данных Уровень «новичок»

Цель настоящей памятки – познакомить читателей с основами компьютерной грамотности и безопасности при работе с важными документами.

Настоящая информация не является исчерпывающей, поэтому мы будем рады вашим комментариям, вопросам и предложениям!

С любовью, БОСС ^^

Часть 1 Как обезопасить свой компьютер/ ноутбук/ планшет/ флешку



Всегда нужно исходить из того, что доступ к вашим данным рано или поздно получают посторонние. Флешку можно потерять, компьютер может перестать работать. Опустим печальные истории о воровстве документов, копировании личной информации и использовании ее против вас. Как говорить: «Береженого и Бог бережет!»

Поэтому давайте вспомним и разберем простые пункты компьютерной грамотности и безопасности.

1. Не использовать одну УЧЕТНУЮ ЗАПИСЬ для всех пользователей компьютера, тем более с правами администратора.

2. Использовать ПАРОЛЬ ДЛЯ ВСЕХ учетных записей пользователей компьютера. Запретить гостевой вход в систему.

2.1. В идеале пользователи не должны обмениваться своими паролями даже при полном доверии друг другу.

2.2. Не стоит пытаться придумать и запомнить пароль, который читается с трудом, вы его забудете быстро и легко. Используйте:

- короткую фразу;
- в которой несколько букв заменены цифрами;
- она может иметь или не иметь смысл;
- содержать или не содержать ошибки в словах.

Например, «Жм8ут галбши офигенн1» (Жмут галоши офигенно), «Бур9 мгл0ю неб0 кр0ет» (Буря мглою небо кроет), «С0нца светет 9рка» (Солнце светит ярко).

Помните, что лучше допустить одну ошибку, заменить одну и ту же букву одной и той же цифрой. Со временем сложный пароль вы-то вспомните, а какие ошибки допустили и цифры использовали, может остаться тайной.

3. Потратить некоторое время на РАЗГРАНИЧЕНИЕ ДОСТУПА.

Ограничения доступа должны быть максимально жёсткими, но при этом достаточно свободными для комфортной работы пользователей. Чтобы задать правила доступа к ресурсу (например, к папке, диску) (см. Приложение 1 в конце) в ОС начиная с Windows XP достаточно открыть свойства папки и во вкладке «Безопасность» нажать кнопку «Изменить». Задавать их можно как для конкретных пользователей поименно, так и для групп.

Например, пусть все члены семьи пользуются одним компьютером и для каждого настроена отдельная учетная запись, при этом имеется группа “Неопытные пользователи”, куда входят Мама и неграмотный по малолетству Петя. Имеет смысл разрешить пользователю Вася полный доступ к папке “Васина папка”, а группе “Неопытные пользователи” и пользователю Вася разрешить просмотр содержимого папки “Семейные фотографии”. В таком случае мама и Петя не смогут просмотреть или повредить Васиные файлы, бездумно согласившись на установку вредоносных программ от своего имени.

4. Использовать программные сетевые экраны (firewall) или комплексы интернет-безопасности (internet security suite) при работе на компьютере, подключенном к сети.

В Интернете полно людей и автоматических сканеров, постоянно ищущих компьютеры, к которым можно подключиться и использовать уязвимости ПО для своих целей. Провайдер и домашний маршрутизатор могут блокировать часть входящих подключений, но при работе с важными данными не следует полагаться на них полностью.

Выбор имеется, бесплатных хватает:

- ZoneAlarm (про настройку можно прочитать здесь <http://sonikelf.ru/zashhishhaemsya-ot-xakerov-chervej-i-prochej-shushery/>), только

качать программу лучше с сайта производителя - <http://www.zonealarm.com/security/en-us/anti-virus-spyware-free-download.htm>),
- Comodo Firewall (настройка и установка описаны здесь <http://forums.comodo.com/10551086108810911089108910821080-russian-b73.0/-t99333.0.html>).

Можно посмотреть Outpost Security Suite free или уточнить у гугла похожие утилиты.

5. Последний рубеж защиты – ШИФРОВАНИЕ, оно может спасти, когда важные данные уже попали не в те руки.

Выбор инструмента шифрования зависит от объема информации и её характера. В случае если вы хотите быстро защитить один или несколько документов, которые редко будут изменяться, создайте архив с паролем. Вам поможет бесплатная утилита 7-zip (см. Приложение 2 в конце).

Также для шифрования отдельных файлов можно воспользоваться бесплатной утилитой AxCrypt. Скачать можно здесь: <http://www.axantum.com/axcrypt/Downloads.aspx>. Как использовать в работе посмотреть здесь: <http://www.youtube.com/watch?v=i7NX3mO2Qbo>

При необходимости частого чтения/изменения документов лучше подойдет вариант с созданием шифрованного контейнера на жестком диске, который после подключения (и единовременного ввода пароля) отображается в системе как еще один жесткий диск, на который можно сохранить несколько документов и изменять их не задумываясь о шифровании.

Настоятельно советуем использовать TrueCrypt. Скачать можно здесь: <http://www.truecrypt.org/downloads>. Информация по использованию: <http://bloginfo.biz/truecrypt-part-one-base-knowledge.html>. В конце работы или при экстренной необходимости такой диск можно отключить, и без повторного ввода пароля содержимое прочитать не удастся. Программу можно использовать и для шифрования флешки. Как это сделать смотреть здесь: <http://habrahabr.ru/post/53720/>

6. Не распространяться об ИМЕЮЩЕЙСЯ у вас ценной информации и используемых средствах обеспечения её сохранности.

Злоумышленнику добраться до информации без таких сведений в разы сложнее, чем когда он наверняка знает что искать и какие механизмы защиты предстоит обойти.

7. Не хранить определенную информацию, а ЗАПОМИНАТЬ И ВИДОИЗМЕНЯТЬ ЕЕ.

Не стоит полагаться только на вышеуказанные программы, т.к. всегда есть вероятность того, что вы по неосторожности скажете свой ключ, или злоумышленник применит старый надежный терморектальный криптоанализ. Давайте договоримся хранить информацию только ту, которая действительно важна и может забыться. НЕ советуем хранить в любом виде и формате:

- пароли. Как легко выбрать и запомнить пароль описано выше;
- имена и телефоны всех лиц, которые не хотят, чтобы о них знали в целях безопасности. Этим людей всегда можно найти вк, связаться по мылу! В случае если нужно пометить их контакты, используйте другое имя. Конечно, кому надо, тот пробьет номер и узнает личность, но вот те, кто взял ваш телефон/ ноут и увидел незнакомую фамилию, не заострит внимание на контакте.



Часть 2

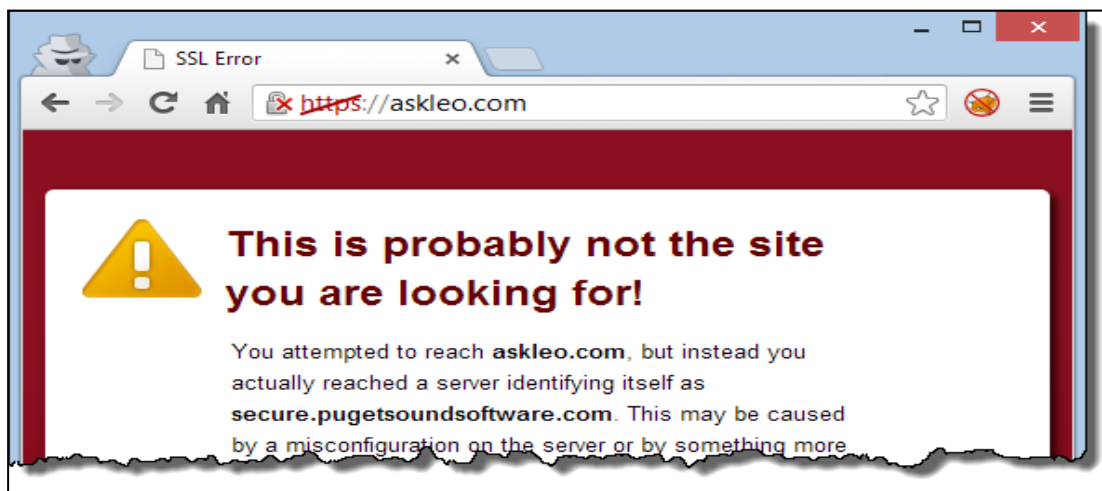
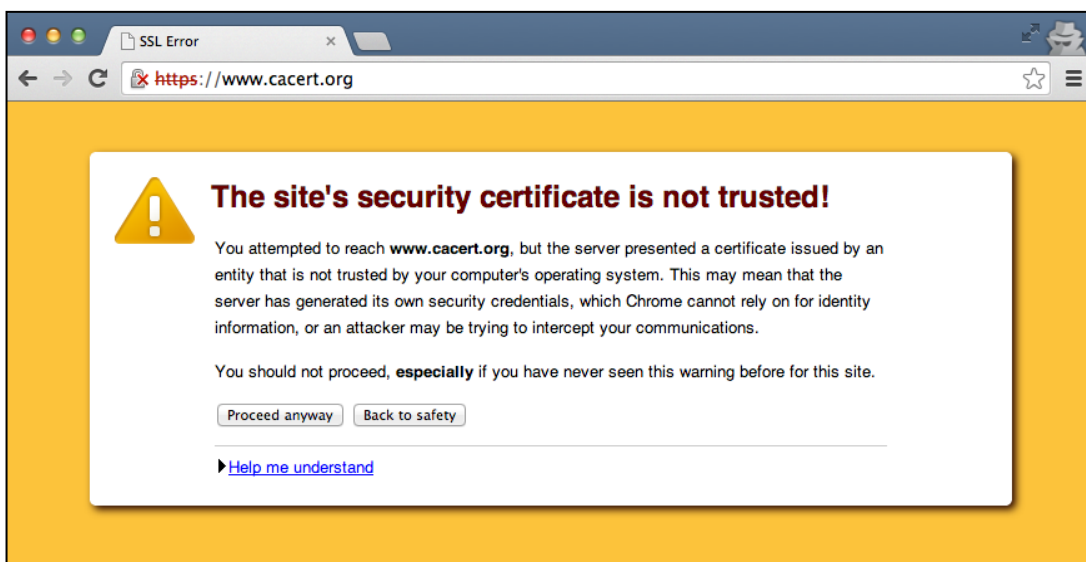
Как обезопасить себя в интернете



1. Используйте https.

Https – протокол передачи данных между браузером и сервером, при использовании которого данные шифруются в обоих направлениях. Основное его назначение – защитить канал связи от прослушивания и изменения передаваемых данных (т.н. man-in-the-middle attack). Это возможно в ситуациях, когда злоумышленник может иметь доступ к телекоммуникационному оборудованию (недобросовестный провайдер, любая публичная точка доступа), т.е. практически всегда. Ценные данные (номера кредитных карточек, логины/ пароли и т.п.) всегда должны передаваться по https, к счастью, в основном пользователям не нужно беспокоиться о включении https, потому что оно иницируется на стороне сервера. Однако следует взять за правило всегда перед вводом ценных данных удостоверяться в

том, что в данный момент используется безопасное подключение. Об этом может свидетельствовать префикс `https://...` в адресной строке браузера и другие визуальные элементы, характерные для каждого браузера ( `https://`,  `https://`). Стоит помнить, даже если вы уверены в защищенности канала связи, владельцы ресурса в интернете всё ещё могут оказаться мошенниками, проверяйте репутацию сайтов и сертификаты. Если при посещении сайта вы видите сообщение, похожее на следующие:



и не уверены в порядочности владельцев, возможно, стоит отказаться от его использования. Бывают случаи, когда одна и та же страница сайта доступна и по незащищенному протоколу, `http` и по `https`, поэтому всегда стоит предпочитать доступ по `https`. Про это легко забыть и проверять каждую страницу на доступность слишком утомительно, к счастью, существуют плагины для браузеров, которые сделают это за пользователя, например `Https`

Everywhere (<https://www.eff.org/https-everywhere>). Они берут на себя заботу о переключении на https всегда, когда это возможно.

2. Сохраняйте АНОНИМНОСТЬ в Интернете

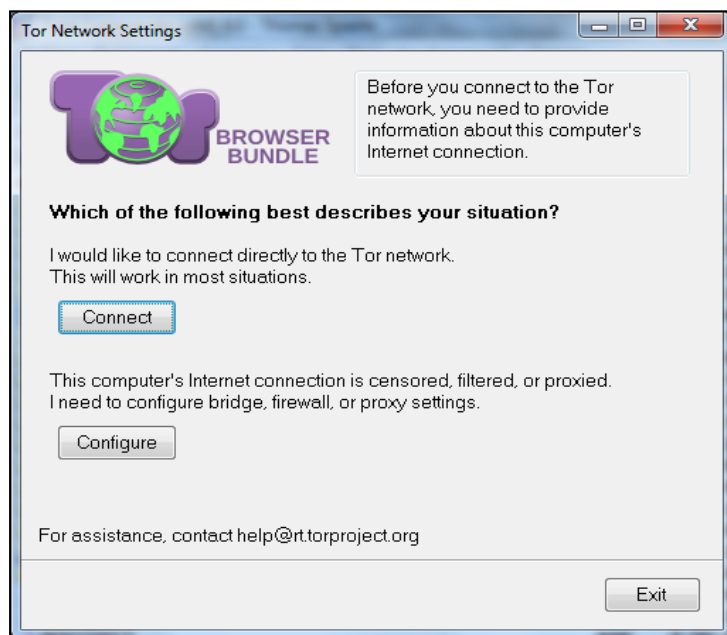
Tor – программа, предназначенная для обеспечения анонимности пользователя при подключении к ресурсам в Интернете (не только веб-сайтам). Благодаря механизму организации соединения через несколько промежуточных прокси-серверов (цепочка Tor), пользователь также получает плюшку в виде возможности доступа к ресурсам (адресат), прямой доступ к которым заблокирован провайдером или на уровне организации. Под анонимностью подразумевается, что Ваш настоящий адрес будет скрыт от узла сети, к которому вы обращаетесь и от всех промежуточных узлов за исключением самого первого. Восстановить цепочку промежуточных подключений через прокси-серверы очень сложно, т.к. каждое соединение шифруется независимо от других. Также использование Tor позволяет скрыть от возможного наблюдателя (Интернет-провайдер), какими данными и с какими ресурсами вы обмениваетесь. Если вам описание работы программы Tor осталось непонятным, то возможно, схема-картинка вам поможет.



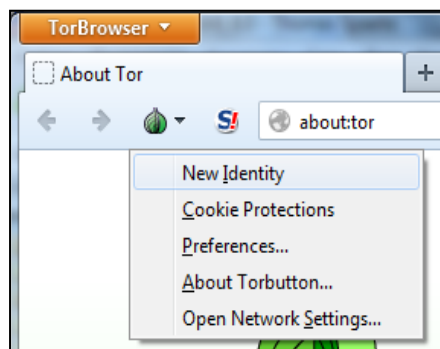
Следует учитывать, что практически каждый желающий, в том числе и вы, может запустить у себя на компьютере сервер Tor, который станет частью единой сети прокси-серверов, и через него будет идти трафик от других пользователей. Это означает, что анонимность сети будет расти при включении в неё большого количества серверов, управляемых разными пользователями.

Самый простой способ начать использовать Tor – скачать Tor Browser (<https://www.torproject.org/projects/torbrowser.html.en#downloads>), после установки в окне настроек выбрать вариант «Подключиться/Connect» или «Настроить/Configure», первый подойдёт в большинстве случаев. Второй

может пригодиться, если вы уже подключены к Интернет через прокси, находитесь за сетевым экраном (firewall) или подключение к сети Tor блокируется провайдером.



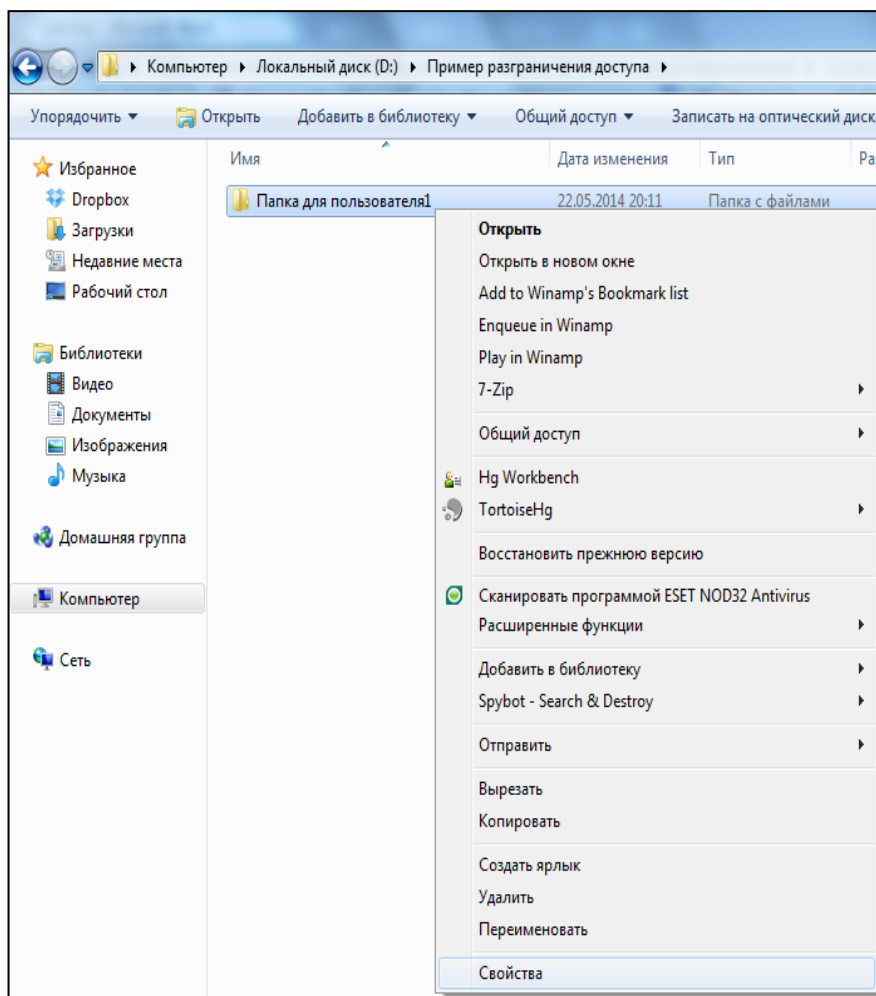
Tor Browser – по сути тот же Firefox, но уже настроенный для использования сети Tor, с установленным плагином HTTPS Everywhere и с дополнительной кнопкой для управления/настройки Tor. Пункт меню «New Identity» используется для смены промежуточных узлов и создания нового маршрута. После выполнения этого действия, для открытых на текущий момент сайтов Вы будете выглядеть как новый пользователь. Если Tor Browser используется не для обхода ограничений, а именно с целью анонимизации, ни в коем случае не авторизуйтесь на ресурсах – зайдя в свой аккаунт в соцсети и т.п. Вы сведёте на нет все усилия Tor по сохранению анонимности.



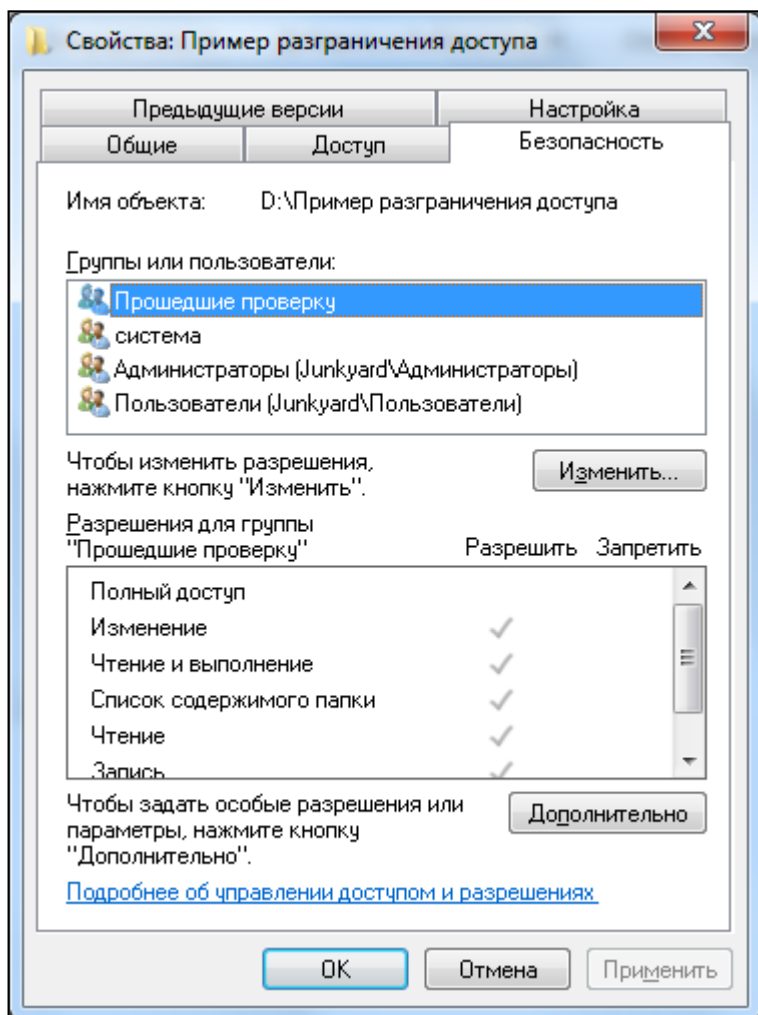
Приложение 1 – разграничение доступа

При создании новой папки к ней применяются те же разрешения/ограничения, которые действуют и для родительской папки (в данном случае для Локального диска D:). Поэтому к только что созданной администратором папке в рассматриваемом примере имеют доступ администраторы и все пользователи кроме гостя (если гостевой вход не отключен). Задача: запретить доступ всем кроме Пользователя 1.

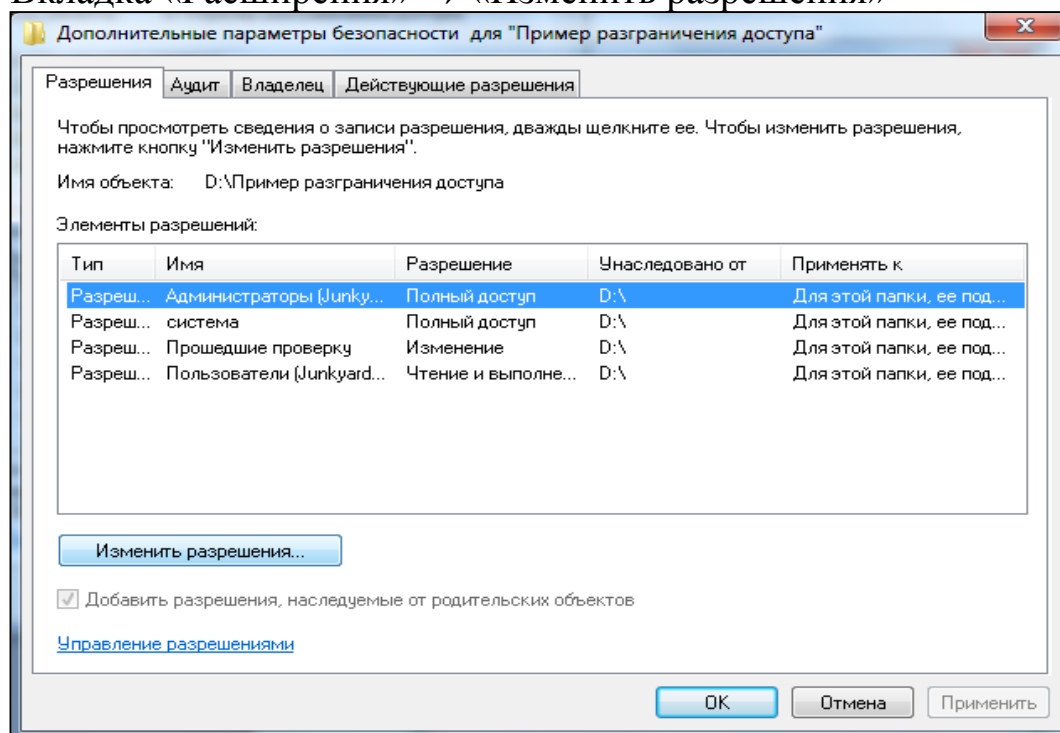
Кликаем правой клавишей мыши на папку, выбираем «Свойства»:



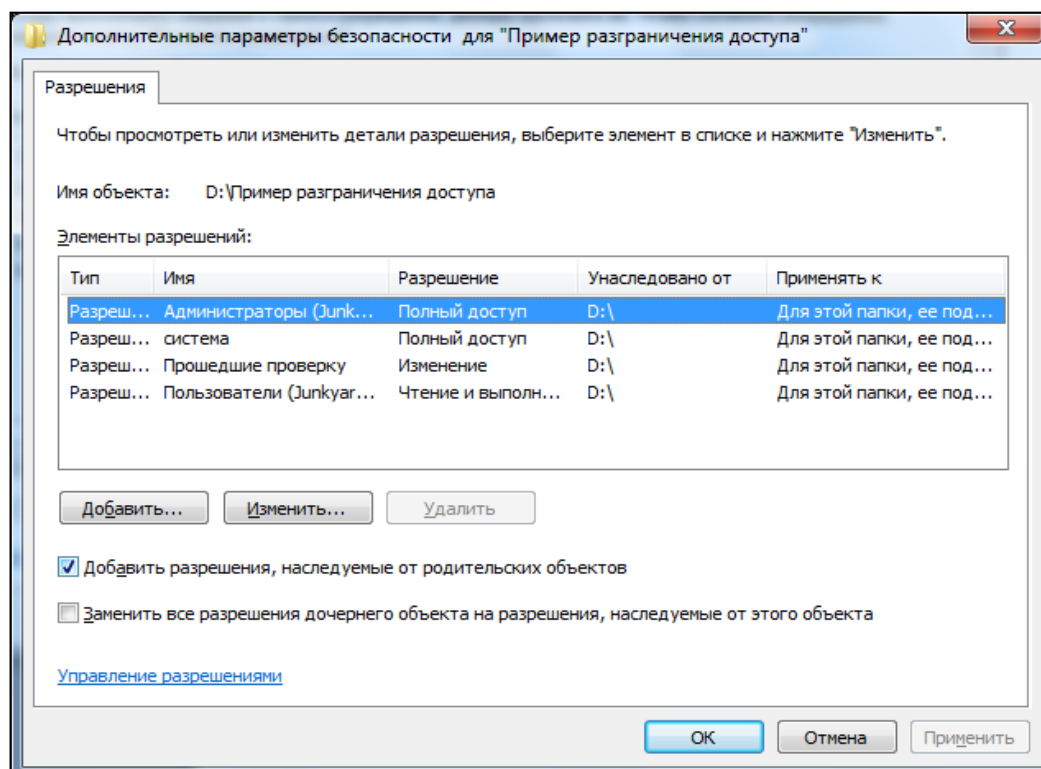
Выбираем вкладку «Безопасность», жмём «Дополнительно»



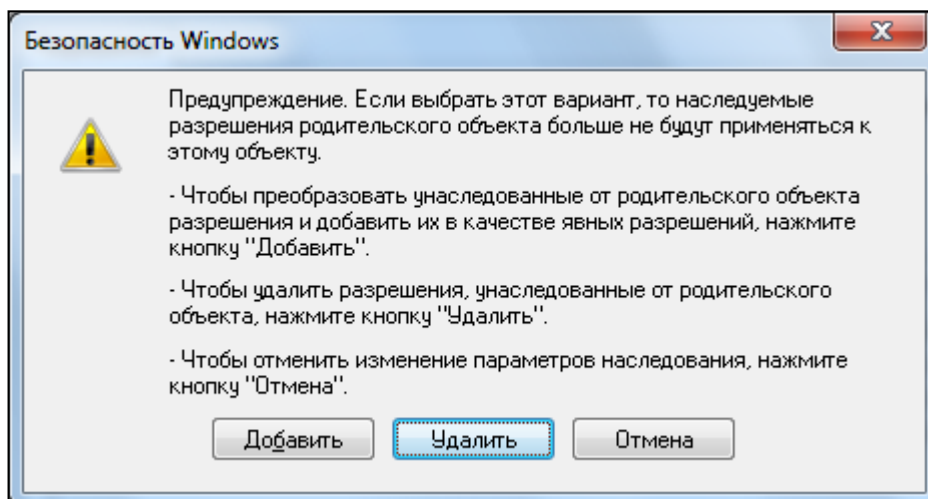
Вкладка «Расширения» → «Изменить разрешения»



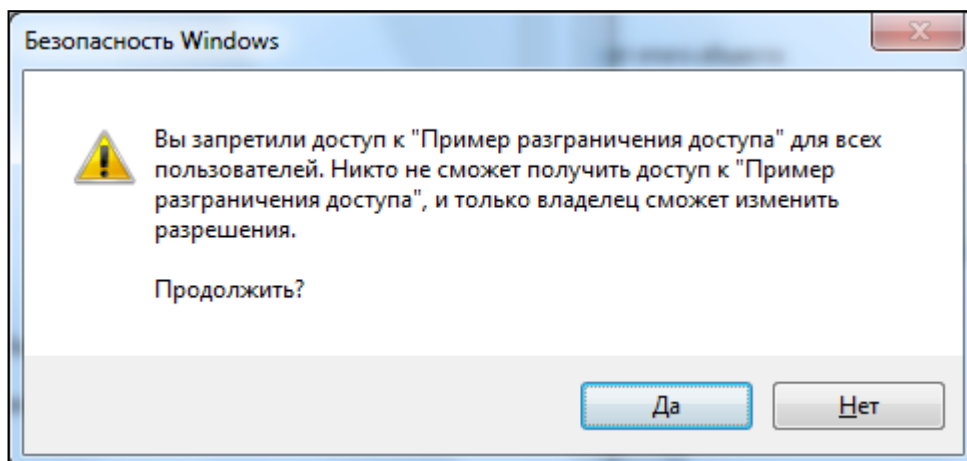
Снимаем флажок «Добавить разрешения, наследуемые от родительских объектов»



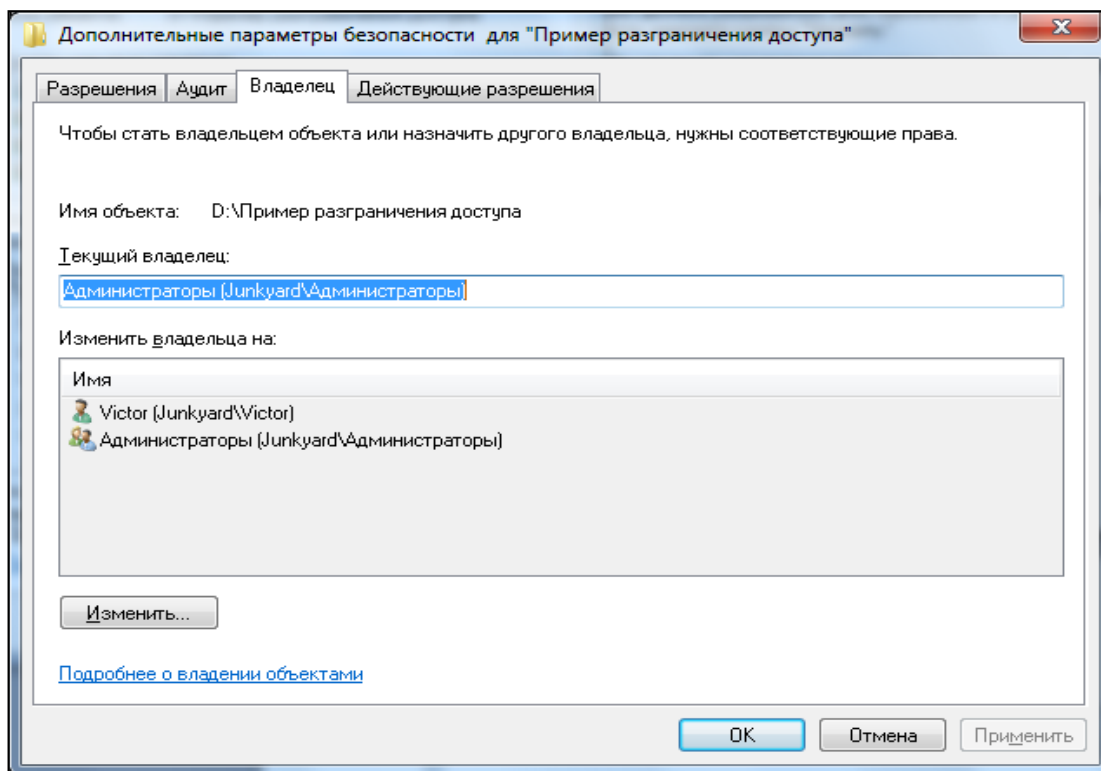
В появившемся диалоге выбираем «Удалить», закрываем предыдущее окно кнопкой «ОК»



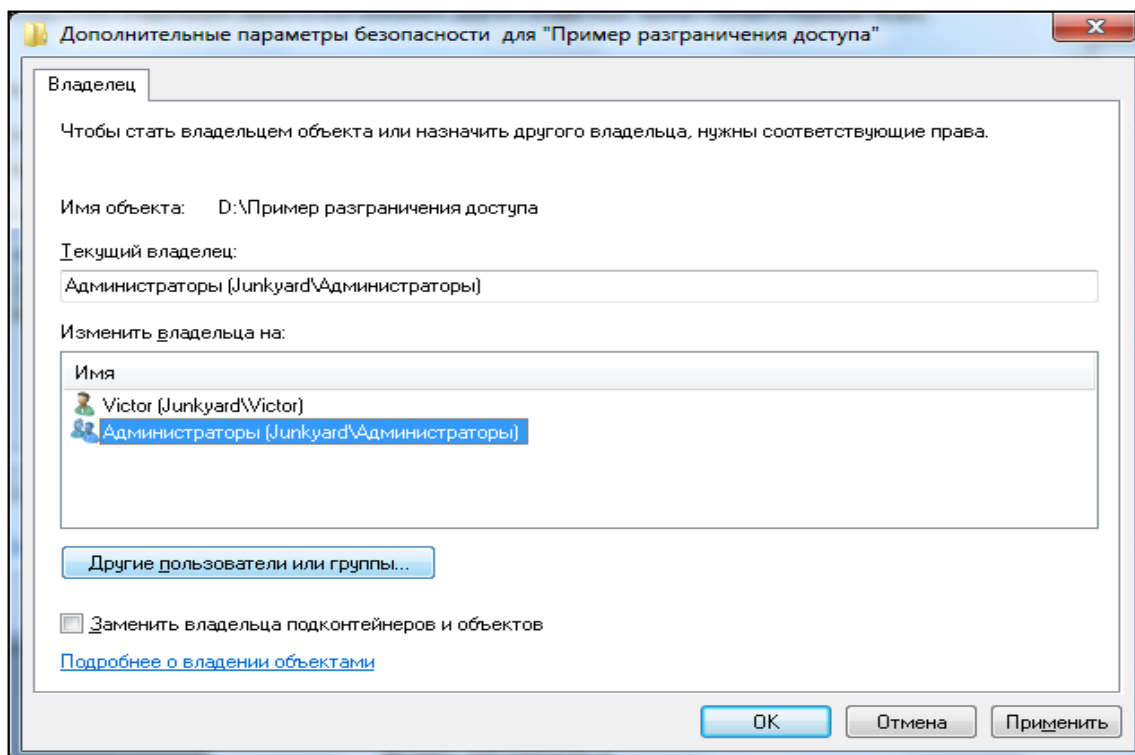
Соглашаемся, остается назначить нового владельца папки.



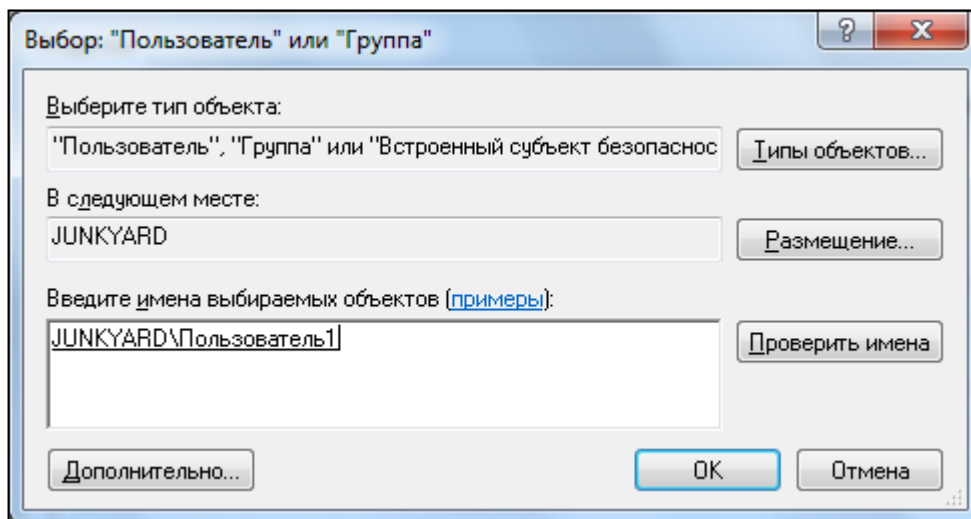
Жмём «Изменить»



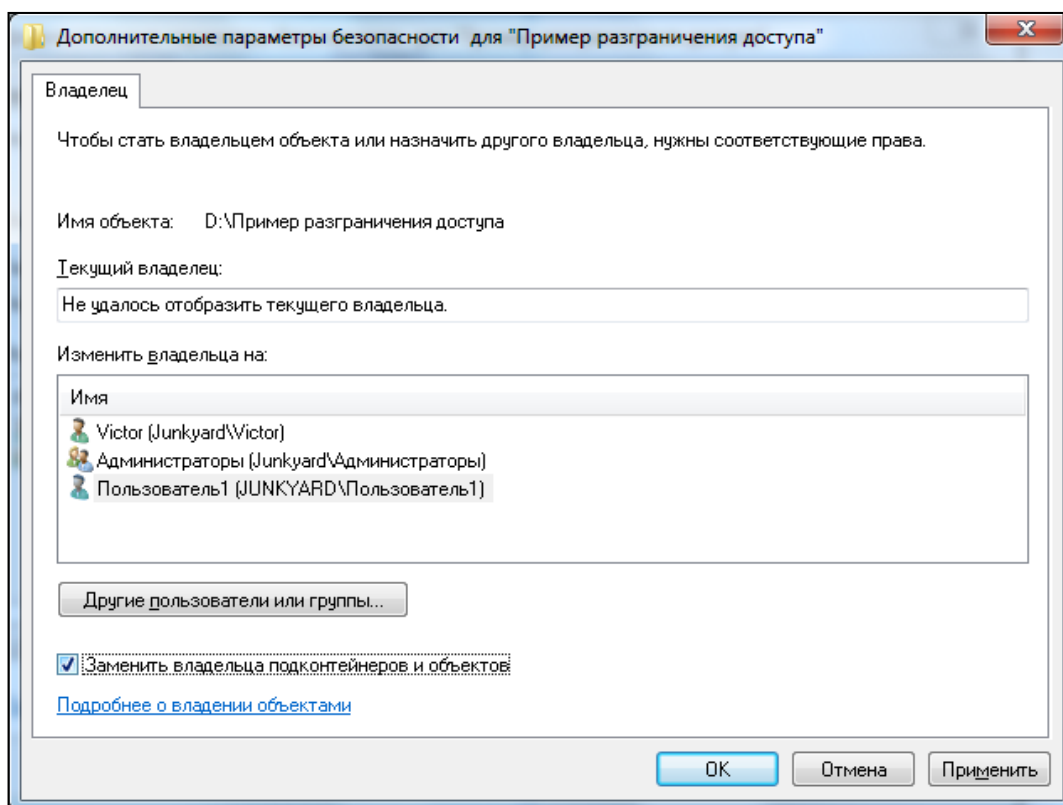
Для выбора нового владельца жмём «Другие пользователи и группы»



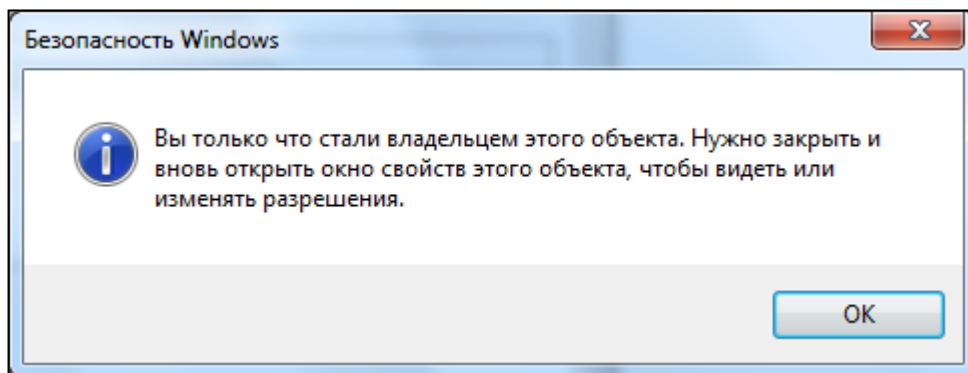
В текстовом поле вводим имя пользователя, который станет владельцем, жмём «Проверить имена», после чего введенное имя будет приведено к виду, принятому в Windows. Жмём «ОК».



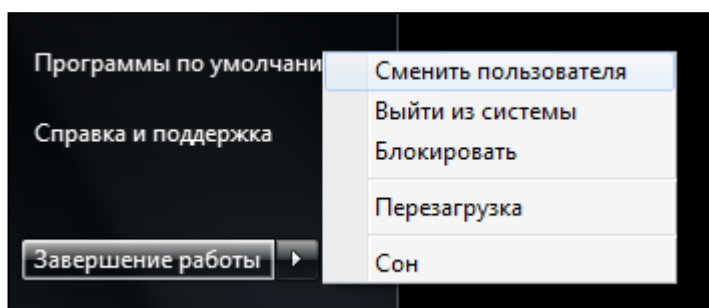
Ставим галочку «Заменить владельца подконтейнеров и объектов» чтобы выбранный пользователь стал также владельцем всех вложенных файлов и папок. Жмём «ОК»

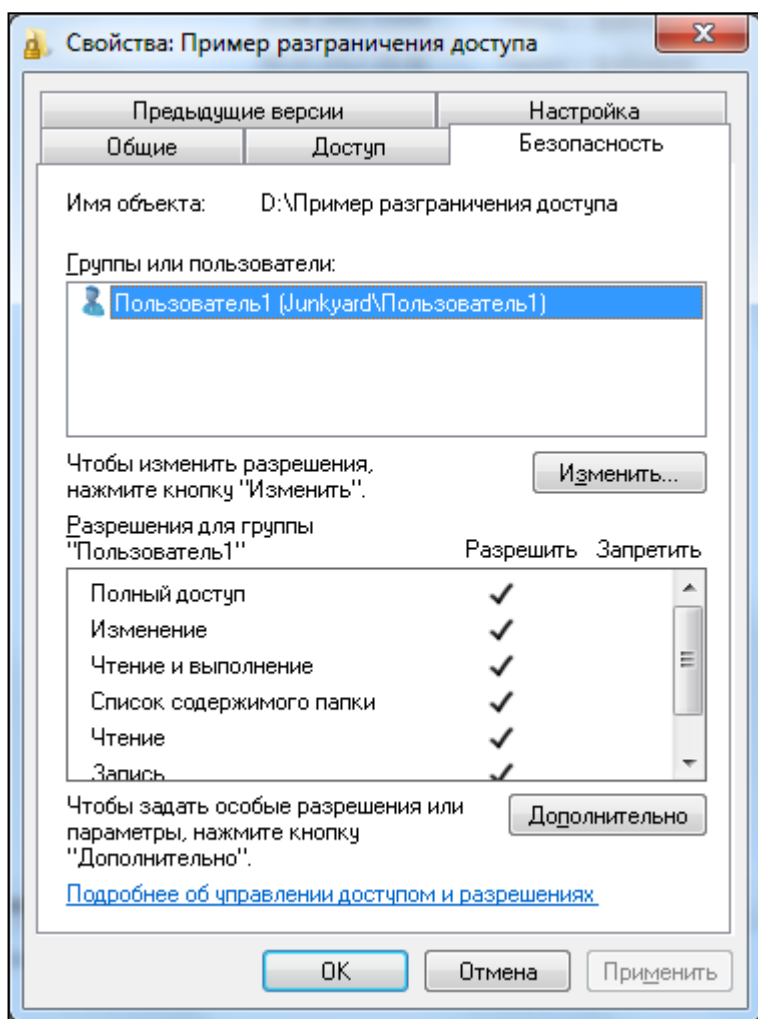


После закрытия последнего диалога папка перестанет быть видна и доступ к ней будет ограничен. Для доступа к ней необходимо войти под учетной записью владельца – Пользователь 1.



Теперь Пользователь1 может в свойствах папки, на закладке «Безопасность» разрешить или ограничить отдельным пользователям или группам доступ к своей папке, нажав «Изменить».

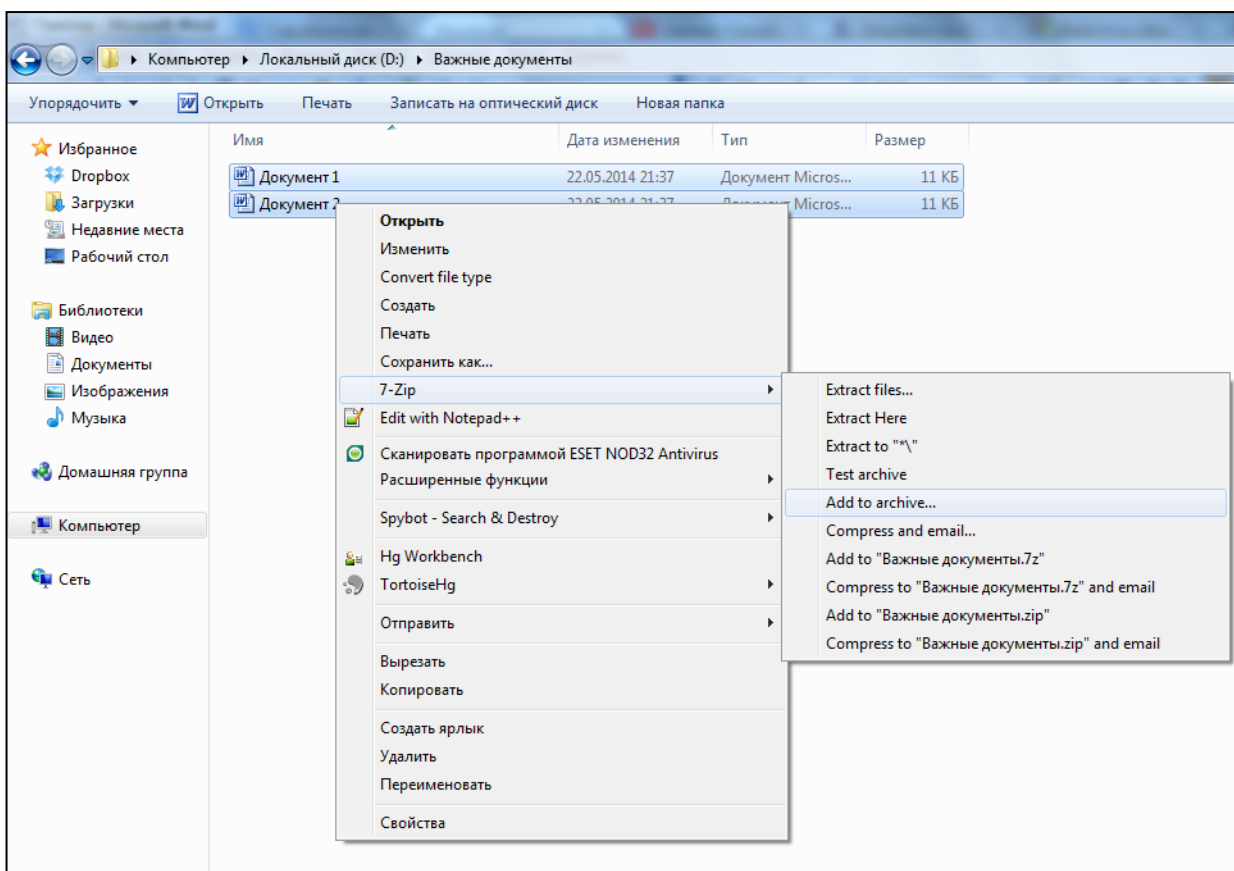




Шагов в этом процессе немало, но главное — понять принципы: разрешения для вложенных папок по умолчанию наследуются от родительской папки, но их можно переопределить вручную; владельцем ресурса может быть пользователь или группа, они могут назначать права доступа для других пользователей; права доступа настраиваются достаточно гибко, помимо прав на чтение и запись файлов можно задать права на просмотр содержимого папки, запуск исполняемых файлов внутри неё, изменение атрибутов папок и файлов.

Приложение 2 – создание архива, защищенного паролем

Скачать 7-Zip можно здесь: <http://www.7-zip.org/download.html>. После установки создавать архивы очень просто: нужно выделить файлы или папки для архивирования и выбрать из контекстного меню (правый клик по одному из выбранных элементов) пункт 7-Zip->Add to archive...



В открывшемся окне можно выбрать формат архива. Формат zip наиболее распространен и с его открытием на другом компьютере скорее всего не возникнет проблем (речь идет не о простоте взлома пароля, а об удобстве обмена файлами в этом формате). Формат 7z имеет небольшое преимущество в степени сжатия данных, но менее распространен. Остальные параметры не имеют большого значения в подавляющем числе случаев. Интерес представляет поле для ввода пароля «Enter password» - при вводе в него ключа (продублированного в поле ниже) содержимое архива будет зашифровано. Помните, длинный легко запоминаемый пароль лучше короткого головоломного, но заменить несколько букв цифрами и другими символами будет не лишним. Encryption method для формата zip позволяет выбрать один из двух методов шифрования: ZipCrypto – широко распространен, поддерживается многими утилитами для упаковки-распаковки; AES-256 – поддерживается несколькими утилитами, но является более устойчивым ко взлому.

Add to Archive [X]

Archive: [...]

Archive format:

Compression level:

Compression method:

Dictionary size:

Word size:

Solid Block size:

Number of CPU threads: / 2

Memory usage for Compressing: 67 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode:

Options

☐ Create SFX archive

☒ Compress shared files

Encryption

Enter password:

Reenter password:

☐ Show Password

Encryption method:

OK Cancel Help