МФТИ it
УПРАВЛЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Методическое пособие

по правилам безопасной работы на персональном компьютере МФТИ

Содержание:

Перечень сокращений:

Корпоративный аккаунт – учетные данные, логин и пароль дают возможность использовать основные информационные системы МФТИ.

Информационная система (далее ИС) – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию. К ИС относятся: 1С, Банк-клиенты, Личный кабинет сайта mipt.ru, кабинет коменданта, почта и многие др.

ОЭАСПС – отдел эксплуатации аппаратных систем и программных средств, тел. 60-62

ПО – программное обеспечение.

ПК – персональный компьютер.

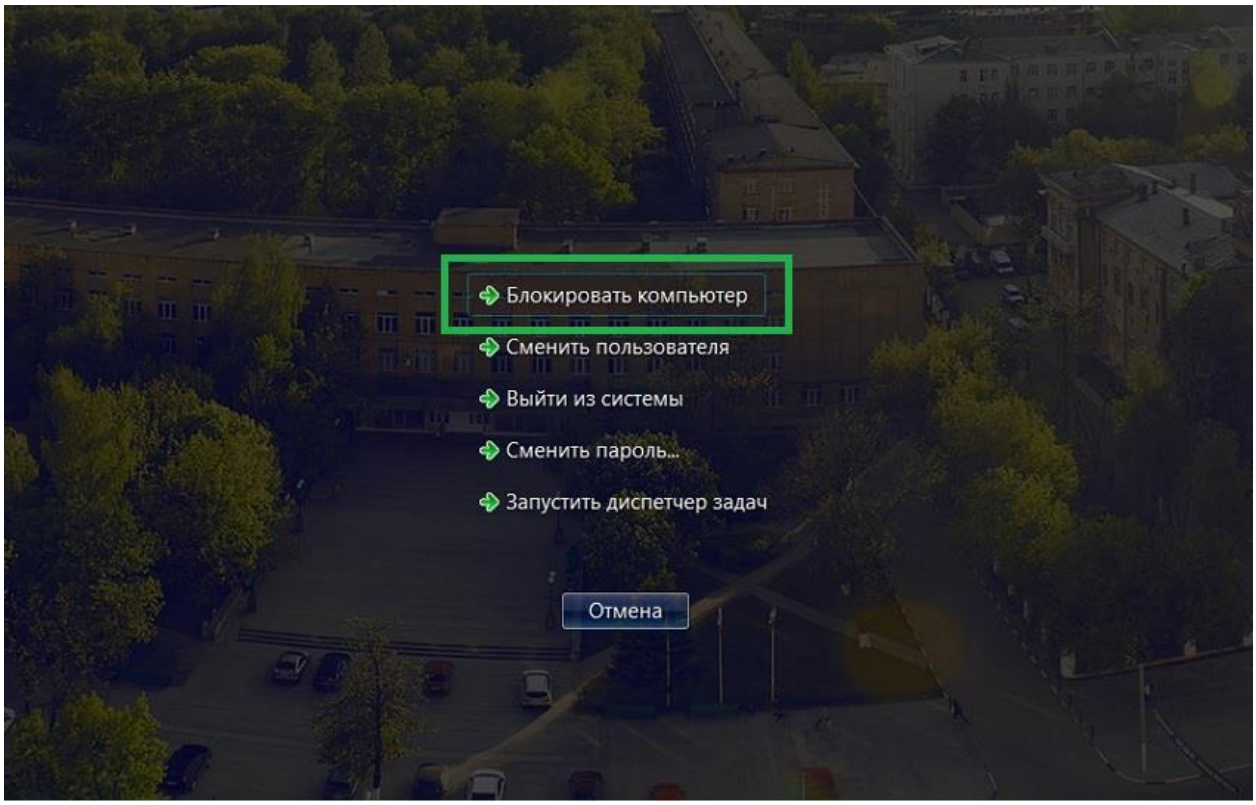
1. Безопасная работа на Компьютере

1.1. Как пользователь, вы несете ответственность за свой компьютер, за данные находящиеся на нём и за доступ к информационным системам в рамках ваших полномочий. Поэтому будьте осторожны.

1.2. Всегда авторизуйтесь на компьютере под собственным Корпоративным аккаунтом, логин пользователя и пароль можно получить в АК517 или КПМ109.

1.3. Никому и никогда и не выдавайте логин и пароль от собственного Корпоративного аккаунта.

1.4. Предотвращайте несанкционированный доступ к вашему ПК и к информационным системам, когда вы выходите из комнаты всегда блокируйте вашу рабочую станцию (на рабочей станции Windows нажмите **Ctrl + Alt + Del** и выберите "**Блокировать компьютер"**).



1.5. Для дополнительной безопасности вы можете также использовать защищенную паролем заставку.

1.6. Не предоставляйте физический доступ к вашему компьютеру сторонним лицам.

1.7. Во время работы часто сохраняйте свою работу. Не оставляйте работу несохраненной, если вы покидаете свою рабочую станцию.

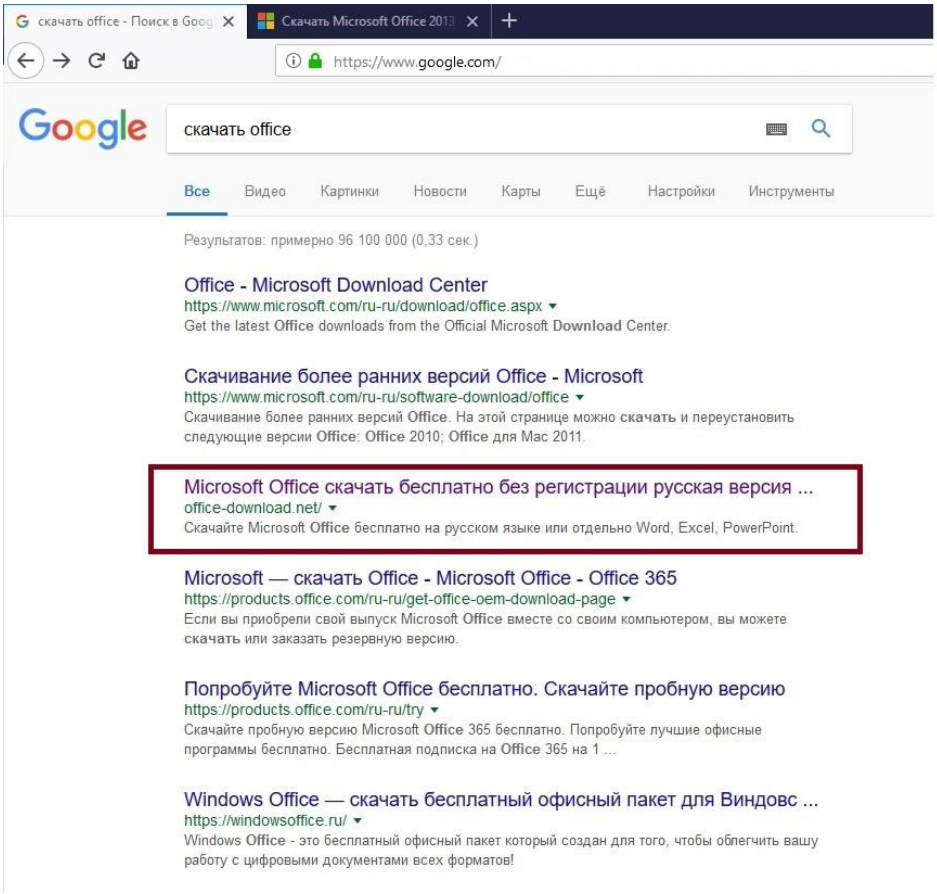
1.8. Сохраняйте все важные данные на диске сетевого сервера (в сетевых папках отдела), из которого ОЭАСПС регулярно создает резервные копии.

1.9. Если жесткий диск рабочей станции или другой носитель данных, например, флешка, карта памяти или CD/DVD-диск, ломается или иным образом изымается из использования, он не должен утилизироваться в мусорном ведре. Необходимо обеспечить его уничтожение в соответствии с инструкциями организации или отдать носитель в ОЭАСПС для уничтожения.

1.10. Только ОЭАСПС может устанавливать компьютерное оборудование (комплектующие ПК) и программное обеспечение на компьютерах.

1.11. Для самостоятельной установки программного обеспечения на компьютер необходимы: лицензионный ключ и уверенность что ПО загружено с официального сайта производителя.

Например, попробуем скачать Office:



Две первых ссылки ссылаются на домен **www.microsoft.com** – как известно это официальный адрес компании Microsoft производителя ПО Office и Windows.

Третья ссылка предлагает скачать приложение бесплатно и без регистрации, и ссылается на домен **office-download.net** – очевидно, что этот сайт с приложениями заражёнными вирусами (троянами, майнерами, шифровальщиками и тд и тп). Скачивать с подобных сайтов ПО и устанавливать их на ПК строго запрещено.

1.12. В конце рабочего дня, выйдите из рабочих программ 1С, личные кабинеты, Office и других. Выключите компьютер, в соответствии с инструкцией ОЭАСПС “пользователя персонального компьютера МФТИ” и инструкциями ГОиЧС.

2. Безопасная работа в Информационных системах

2.1. Для ИС необходимы права доступа. Ваше право доступа является личным и это связано конкретно с вашими должностными обязанностями. Обращайтесь с учётной записью от ИС (логином и паролем) так же, как и с вашей собственной банковской картой и её PIN-кодом.

2.2. Не передавайте пароли или PIN-коды от ИС другим лицам - даже системным администраторам. Отвечайте отказом по всем запросам и просьбам, связанным с вашими паролями от ИС или доступом к системе прав ИС.

2.3. Периодически меняйте свои пароли. Измените пароль от ИС сразу, когда вы подозреваете что он мог быть раскрыт.

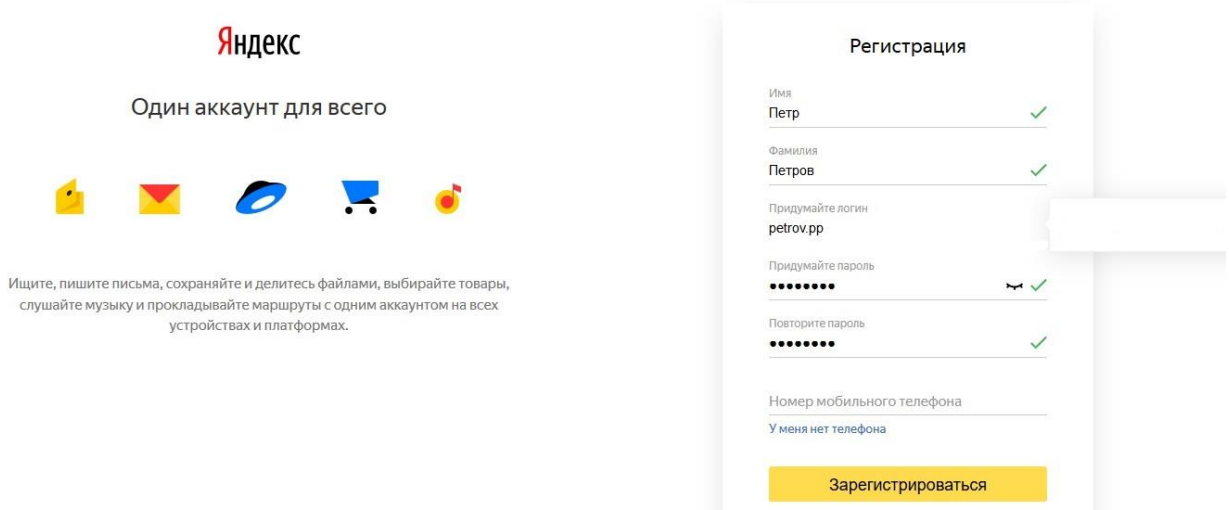
2.4. Убедитесь, что ваши пароли от ИС достаточно сложны. Избегайте использования в качестве пароля знакомых односложных повседневных слов, дат рождений, имён близких. Хороший пароль должен иметь заглавные и малые буквы, цифры и даже специальные символы. Не все ИС принимают специальные символы. Хороший пароль легко запомнить со временем, и сложно подобрать злоумышленнику.

2.5. Не записывайте пароли в том месте, где они могут быть легко найдены (например, под клавиатурой, на стикере приклеенном к монитору или на рабочем столе в текстовом файле).

2.6. Иногда в определенных ситуациях в ИС необходимо использовать общие учетные записи. Использование общих учетных записей разрешается только с разрешения владельца. Пароль общей учетной записи должен быть изменен, когда один из пользователей, имеющих доступ увольняется (или переходит в другой отдел) или есть подозрения, что кто-то, не принадлежащий к подразделению, узнал логин и пароль. Пароли в любом случае должны меняться достаточно часто.

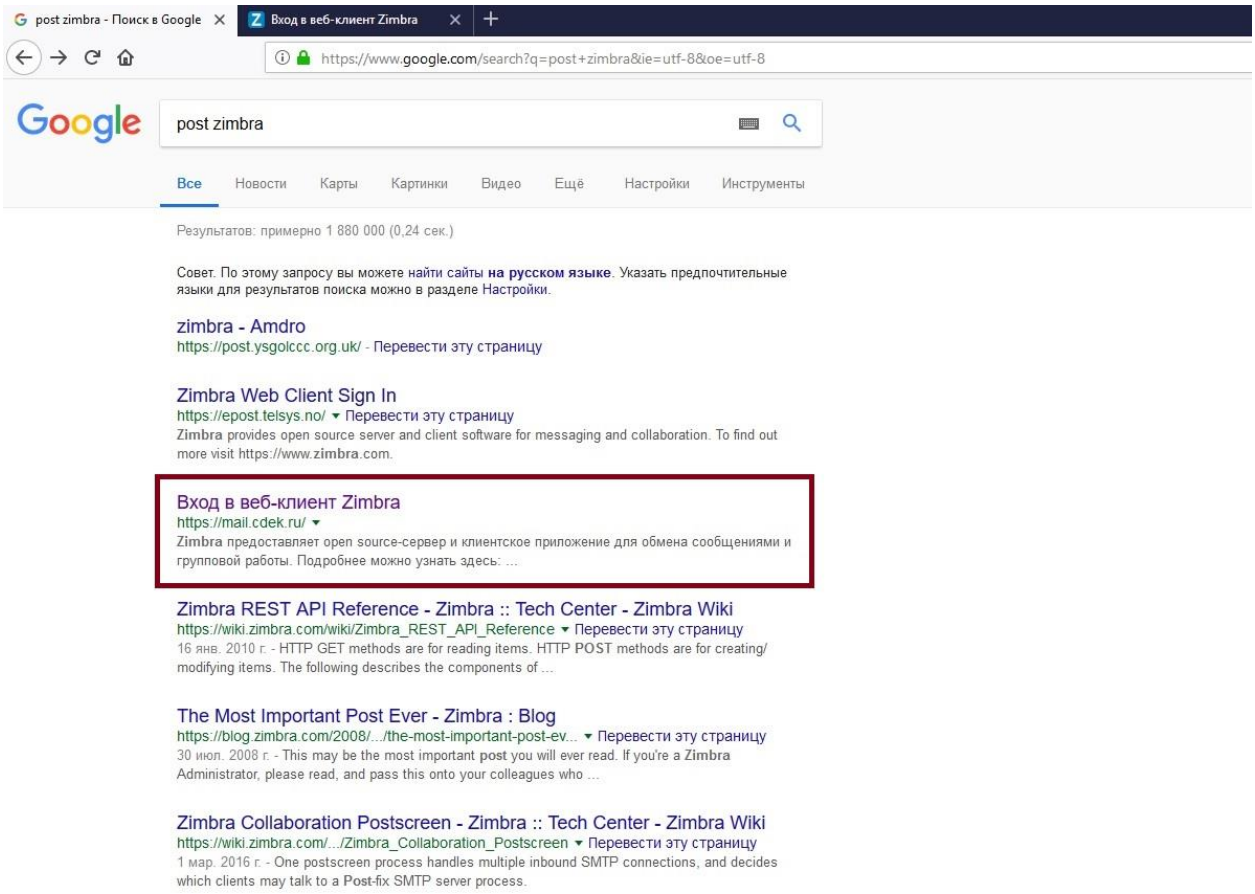
2.7. Не используйте учетную запись пользователя или пароль, выданные для доступа к ИС МФТИ, для регистрации внешних интернет-услуг.

Например, в данном случае при регистрации аккаунта на Яндекс **недопустимо** использовать Логин и пароль от Корпоративного аккаунта.

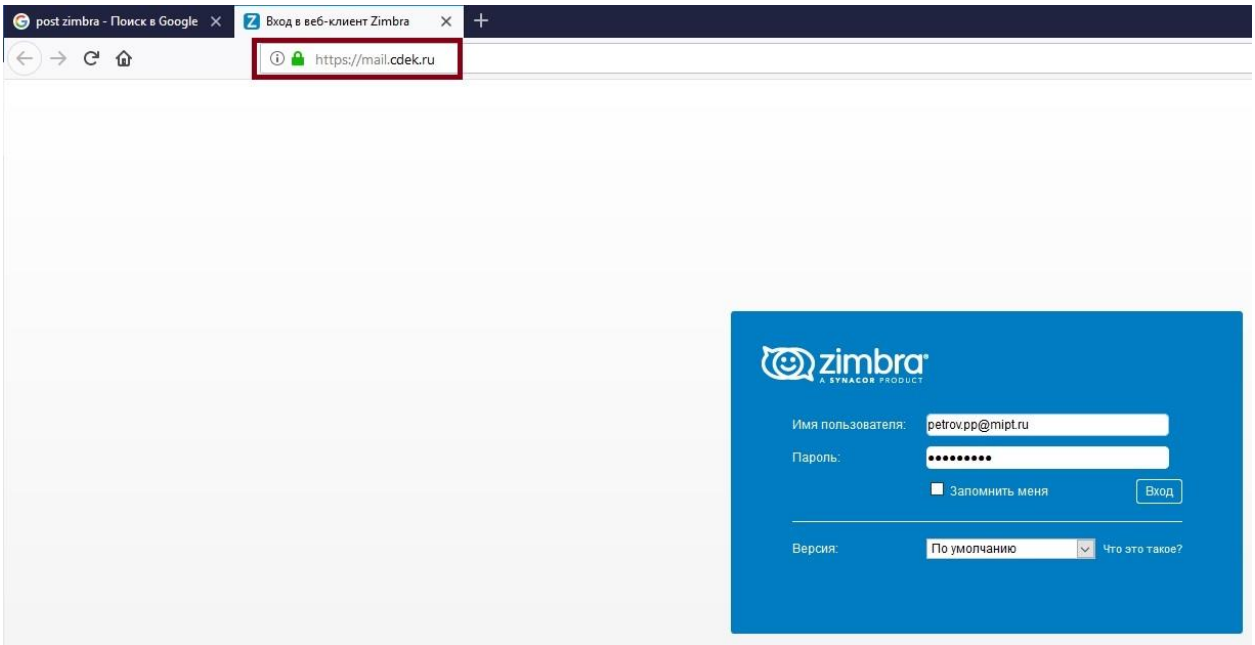


2.8. Так же не допустима попытка авторизация на сторонних серверах под учетной записью МФТИ

2.9. Если сотрудник не знает web адреса почтового сервера МФТИ, но помнит ключевое слово Zimbra, то он может попробовать найти web адрес в поиске по запросам «почта Zimbra» или «post Zimbra», например:



Идем по ссылке **Вход в веб-клиент Zimbra**. Пытаемся авторизоваться. Не получается. Обратите внимание на адрес в адресной строке!



Это адрес почтового сервера Zimbra Курьерской службы доставки СДЭК в Москве. На что следует обращать внимание – на адрес сервера ИС. Адрес почтового сервера МФТИ **post.mipt.ru**, в большинстве адресов ИС МФТИ должен по крайней мере встречаться кусок "**mipt.ru**".

3. Безопасная работа с почтой и в сети Интернет

3.1. Интернет и электронная почта - хорошие инструменты как для поиска информации, так и для общения. Однако вы должны помнить, что электронная почта или интернет не имеют защиты сами по себе; информация перемещается в незашифрованном виде общественной сети. E-mail и интернет следует использовать с осторожностью.

3.2. Интернет и корпоративная электронная почта предназначены только для официального использования. Для личных целей используйте свой частный адрес электронной почты.

3.3. Запрещается отправлять конфиденциальную информацию через Интернет без необходимого сильного шифрования информации. Такие сообщения и отправляемые документы должны быть зашифрованы с использованием продуктов и технологий, одобренных ОЭАСПС.

3.4. Научитесь правильно использовать продукты шифрования, чтобы не было непреднамеренно отправленной незашифрованной информации.

3.5. При загрузке программ через Интернет всегда старайтесь подтвердить надежность программного обеспечения и его источника.

3.6. Если вы временно используете компьютер другого человека, не забудьте очистить кеш интернет-браузера и cookies. Если необходимо, обратитесь за помощью в ОЭАСПС.

3.7. Помните, что вы несете ответственность в соответствии с вашими служебными обязанностями, за любое связанное с работой электронное письмо, которое может быть отправлено на вашу личную электронную почту.

3.8. Использование электронной почты, отличной от корпоративной электронной почты (например, электронных почт mail, rambler, gmail) разрешается только с согласия начальства подразделения.

3.9. Вложения электронной почты могут содержать вредоносное ПО (вирусы, черви, троянские программы или шифровальщики). Работайте осторожно со всеми не типичными сообщениями электронной почты, особенно с подозрительными вложениями.

Например, файл вложения **Годовой отчёт.exe** в письме может быть либо самораспаковывающимся архивом, либо, что более вероятно, троянской программой или вирусом.

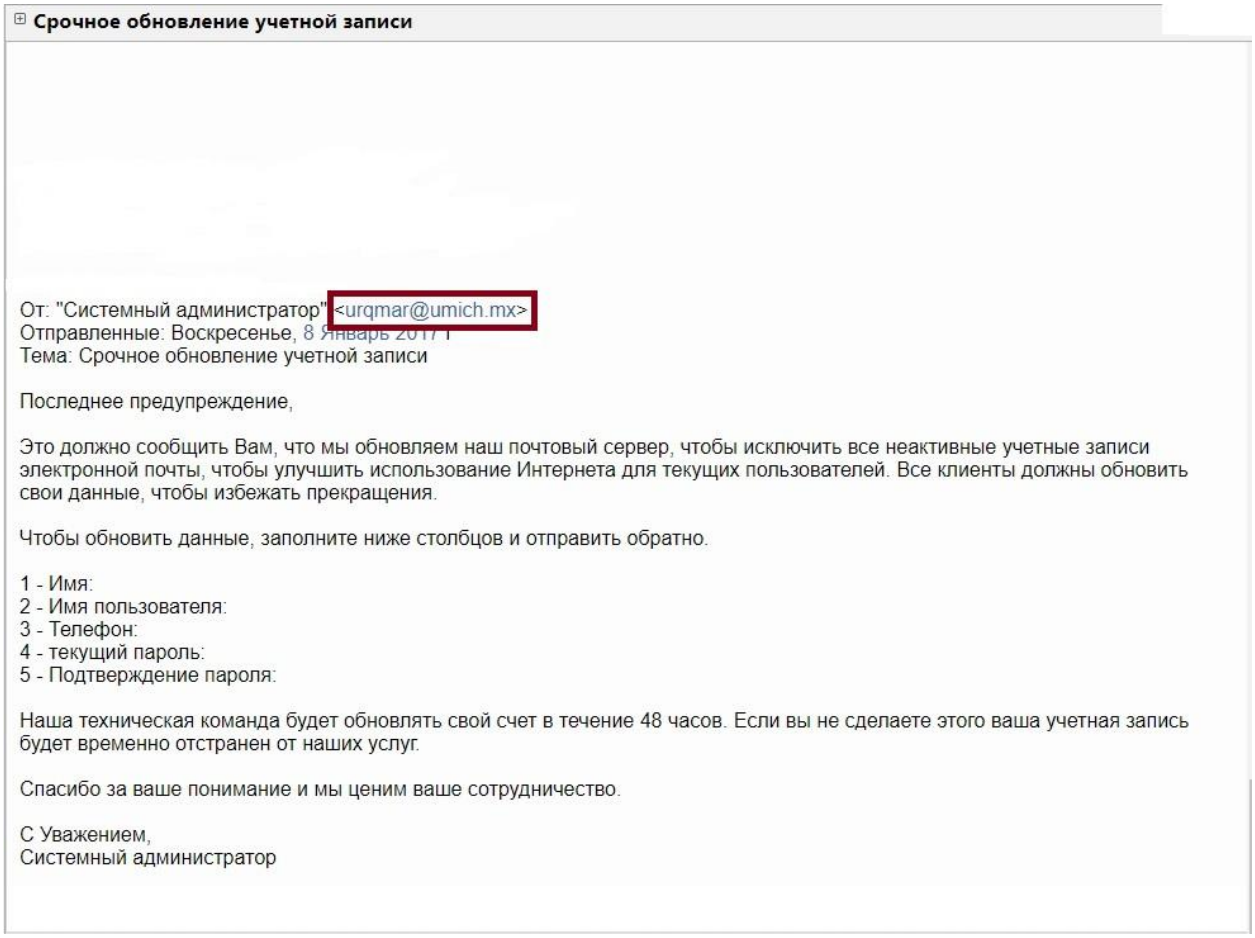
3.10. Не открывайте подозрительные сообщения, и тем более не пытайтесь открыть вложения к ним. При необходимости свяжитесь с ОЭАСПС.

3.11. Не передавайте свой рабочий адрес электронной почты третьим лицам, кроме лиц, связанных с вашей работой.

3.12. Обращайте внимание на достоверность электронной почты. Сообщение электронной почты может быть прислано откуда угодно, кроме указанного отправителя в поле "От" ("From"). Вирусы также могут отправлять электронную почту без каких-либо действий пользователя.

3.13. Остерегайтесь «фишинговых писем», которые просят вас вводить идентификаторы пользователей и пароли для служб, которые выглядят аутентичными. В подобных случаях никогда не высылайте свои личные данные, логин и пароль от почты и других ИС. При необходимости свяжитесь с ОЭАСПС.

3.14. В данном письме некий “Системный администратор” предупреждает что будет обновлен наш корпоративный почтовый сервер и требует выслать на обратный адрес не только логин и пароль, но ещё и номер телефона, для того чтобы якобы обновить учетную запись.



Срочное обновление учетной записи

От: "Системный администратор" <urqmar@umich.mx>
Отправленные: Воскресенье, 8 Январь 2017 г
Тема: Срочное обновление учетной записи

Последнее предупреждение,

Это должно сообщить Вам, что мы обновляем наш почтовый сервер, чтобы исключить все неактивные учетные записи электронной почты, чтобы улучшить использование Интернета для текущих пользователей. Все клиенты должны обновить свои данные, чтобы избежать прекращения.

Чтобы обновить данные, заполните ниже столбцов и отправить обратно.

1 - Имя:
2 - Имя пользователя:
3 - Телефон:
4 - текущий пароль:
5 - Подтверждение пароля:

Наша техническая команда будет обновлять свой счет в течение 48 часов. Если вы не сделаете этого ваша учетная запись будет временно отстранен от наших услуг.

Спасибо за ваше понимание и мы ценим ваше сотрудничество.

С Уважением,
Системный администратор

На что следует обратить внимание при получении подобных писем:

- Системные администраторы, тех. специалисты по всем ИС МФТИ **никогда** не запрашивают логины и пароли у пользователей, тем более через почту

- “Системный администратор” обезличен, нет ни его имени и фамилии, ни номера телефона в подписи к письму

- почтовый адрес “Системного администратора” имеет домен **umich.mx** это не домен МФТИ. Все администраторы МФТИ имеют почту в доменах **mipt.ru** и **phystech.edu**. И они не будут писать пользователю с почты стороннего, чужого домена.

- ну и часто может насторожить формулировка и постановка предложений в письме, в данном примере видимо использовался машинный перевод на русский с другого языка.

3.15. Если вы получили сообщение электронной почты, принадлежащее какому-либо другому сотруднику, перешлите сообщение правильному получателю и сообщите отправителю правильный адрес электронной почты получателя. Если вы не знаете правильный адрес, сообщите об этом отправителю ошибочного письма. Помните, что вы обязаны сохранить конфиденциальность любого полученного вами сообщения.

3.16. Список рассылки - это список людей, раскрываемый каждому получателю из этого списка, и это может быть личной или конфиденциальной информацией, определяемой

конкретными положениями о раскрытии информации. Вы можете использовать функцию скрытой копии электронной почты если вы хотите предотвратить отображение адресов в списке рассылки получателями.

3.17. Следите за тем, чтобы любое отправленное вами электронное сообщение было отправлено правильным людям и на правильные адреса, в том числе и когда вы используете подготовленные списки рассылки. Избегайте отправки ненужных сообщений электронной почты. Отправка, например, рождественского поздравления загружают как систему электронной почты, так и почтовый ящик получателя.

4. Безопасная работа со съемными носителями информации

4.1. Съемный носитель информации может быть заражён вирусом, поэтому при подключении внешних носителей (флешек, карт памяти, переносных usb дисков) настоятельно рекомендуется проверить носитель с помощью антивируса. На доменных ПК проверка проводится автоматически. Прерывать проверку носителя не рекомендуется.

4.2. Существует большое количество вирусов, предназначенных для повреждения информации на флэшках. Подобные вирусы на зараженном (подозрительном) ПК постоянно загружены в оперативную память и отслеживают порты на предмет подключения съемных носителей. Рабочий съемный носитель подключать к подозрительным ПК нужно только после предварительного бэкапа всех файлов с носителя.

4.3. При подключении рабочей флешки с конфиденциальными данными к подозрительному или внешнему ПК (не принадлежащему корпоративному домену МФТИ) нужно учитывать, что на данном ПК могут быть установлены программы для скрытого копирования информации с флешек. Такие программы сканируют порты USB на предмет подключения съемных носителей и скрыто копируют с них информацию при подключении.

4.4. Испорченные носители нельзя утилизировать – выкинув в мусорное ведро, так как на них могут быть конфиденциальные данные возможные для восстановления. Необходимо обеспечить его уничтожение в соответствии с инструкциями организации или отдать носитель в ОЭАСПС для уничтожения.

5. Безопасная работа с периферийными устройствами (принтеры, сканеры, МФУ)

5.1. При работе на периферийных устройствах (МФУ, сканеры) с документами, содержащими конфиденциальные данные важно искомые документы не забывать в устройстве.

5.2. Сканирование документа с МФУ, содержащего конфиденциальные данные, на внешний личный почтовый ящик (gmail, yandex, mail) не безопасно, так как документ может быть получен третьими лицами.