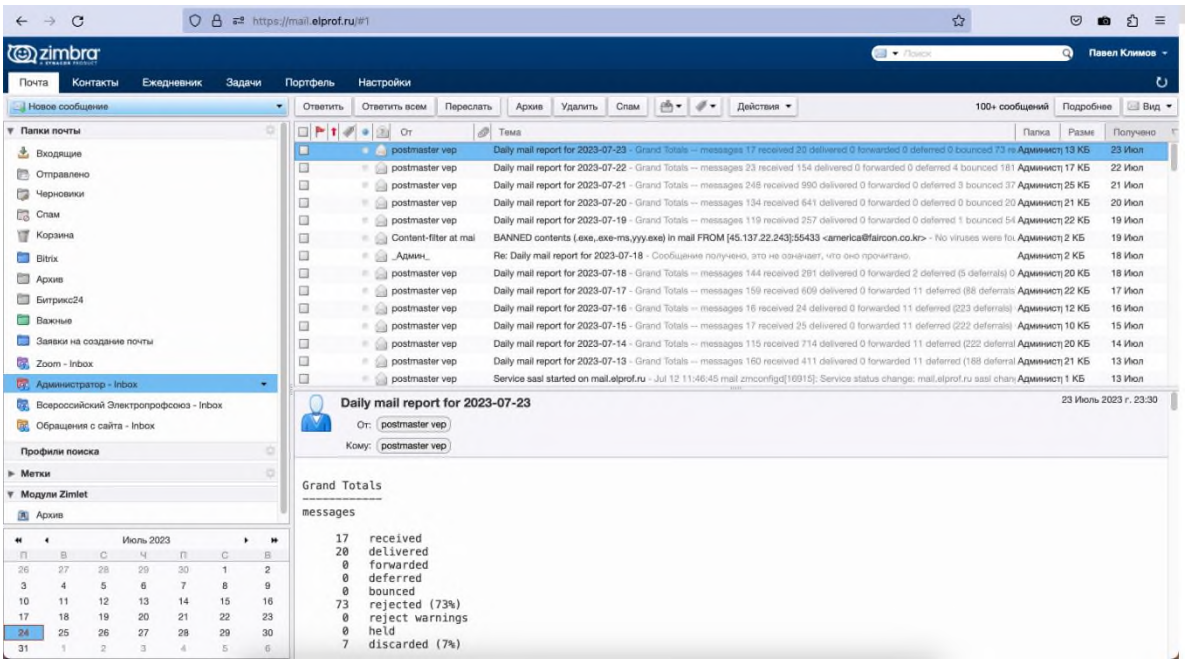
Утверждено
постановлением Президиума ВЭП
от 19.09.2023 № 17-12

ИНСТРУКЦИЯ
по работе с корпоративной почтой в организациях Профсоюза

Zimbra Collaboration Suite (ZCS) – аналог Microsoft Exchange с некоторыми возможностями MAIL.RU, Yandex Mail и т.д.

ZCS предлагается в пяти версиях: Open Source Edition, Consumer Edition, Business Email Edition, Standard Edition, Professional Edition.

Версии Consumer Edition, Business Email Edition, Standard Edition, Professional Edition являются платными, стоимость зависит от версии ПО, в которое входит тот или иной набор функционала и количества пользователей.



Open Source Edition – бесплатная версия с некоторыми ограничениями, но все основные функции работают так же как у Mail.ru, Yandex Mail и других аналогичных сервисов. Данная версия используется в качестве системы обмена документами в ВЭП.

Версии Consumer Edition и Business Email Edition доступны только для хостинг-провайдеров.

В состав **ZCS** входят клиентское и серверное программное обеспечение.

Zimbra Web Client – веб-клиент для совместной работы, поддерживающий email и group calendars. Пользовательский интерфейс Zimbra Web Client построен с использованием технологии AJAX, обеспечивающей всплывающие подсказки, перемещаемые объекты и контекстные меню. Также включены продвинутые возможности поиска и временные зависимости.

Сюда же входят онлайн-документация, модули Zimlet и полноценный интерфейс для администраторов, написанные с помощью Zimbra Ajax Toolkit.

Zimbra Desktop — клиент для совместной работы. Может использоваться в качестве почтового клиента для любого почтового сервиса, поддерживающего протоколы POP и IMAP (протоколы передачи почтовых сообщений в сети Интернет). Клиент доступен на платформах Linux, Windows и macOS.

Zimbra Server — использует несколько СПО-проектов. Он раскрывает SOAP-интерфейс *(SOAP — это **протокол, по которому веб-сервисы взаимодействуют друг с другом или с клиентами**. Название происходит от сокращения Simple Object Access Protocol («простой протокол доступа к объектам»). SOAP API — это веб-сервис, использующий протокол SOAP для обмена сообщениями между серверами и клиентами.)* программирования приложений во всей его функциональности и также является IMAP- и POP3-сервером. Сервер доступен на платформах Linux (Red Hat Enterprise, Fedora, Ubuntu, Debian, Mandriva, SUSE Linux) и macOS.

ZCS совместим как с проприетарными клиентами, такими как Microsoft Outlook и Apple Mail, при помощи проприетарных модулей, так и с открытым Novell Evolution, так что письма, контакты и объекты календаря могут быть перенесены из них в ZCS-сервер. Zimbra также обеспечивает простую двустороннюю синхронизацию со многими мобильными устройствами (Nokia Eseries, BlackBerry, Windows Mobile, iPhone с прошивкой 2.0 и выше).

В любом браузере (программа для работы в Internet - рисунок № 1) в адресной строке необходимо ввести адрес почтового сервера **https://mail.elprof.ru.** Протокол HTTPS необходимо указывать ОБЯЗАТЕЛЬНО!, в противном случае выдаст ошибку **Internal Server Error**, переадресация с незащищённого протокола HTTP отключена в целях безопасности, что бы исключить подмену адреса в строке браузера. Протокол HTTPS имеет 128 битное шифрование данных, которое покреплено специальным ключом безопасности.

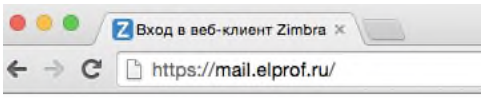


Рисунок № 1

В диалоговом окне необходимо ввести Ваши учетные данные, логин и пароль, в формате указанном на рисунке № 2. Логин вводится без @elprof.ru Пароль вводится в точности, как указан в полученных Вами учетных данных, английскими буквами, на пример - Xc3kHklAs, в поле пароль будут отображаться значки *, или другие символы, используемые в браузере, установленном на компьютере пользователя. Если пользователю необходимо сохранить пароль для того, чтобы каждый раз его не вводить – нажмите галочку в поле «Запомнить меня», которое располагается после полей «Имя пользователя» и «Пароль». Браузер так же может предложить сохранить пароль, если Вы уверены в сохранности полученной информации, можете согласится с предложением сохранить пароль. Стоит обратить внимание, на то, что вход в систему обмена документами брендирован логотипом ВЭП с полным названием организации.

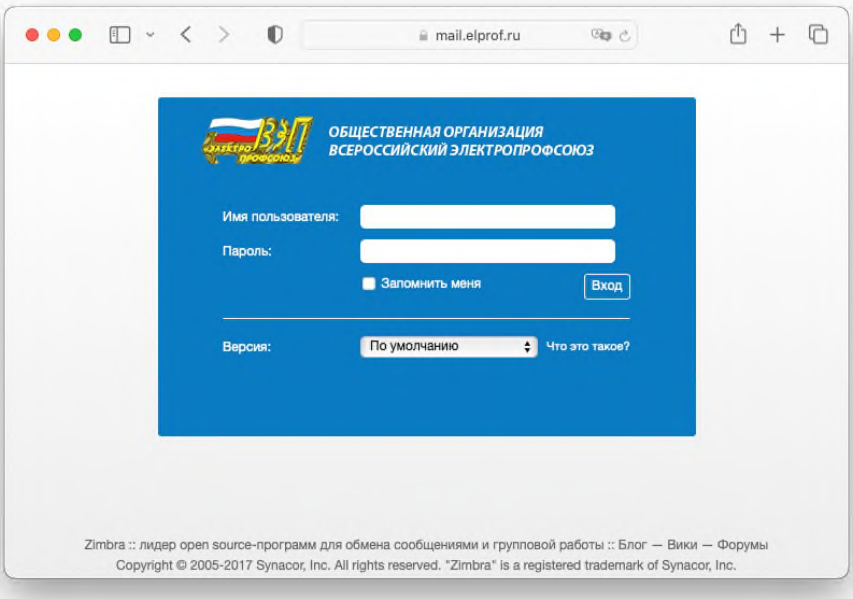
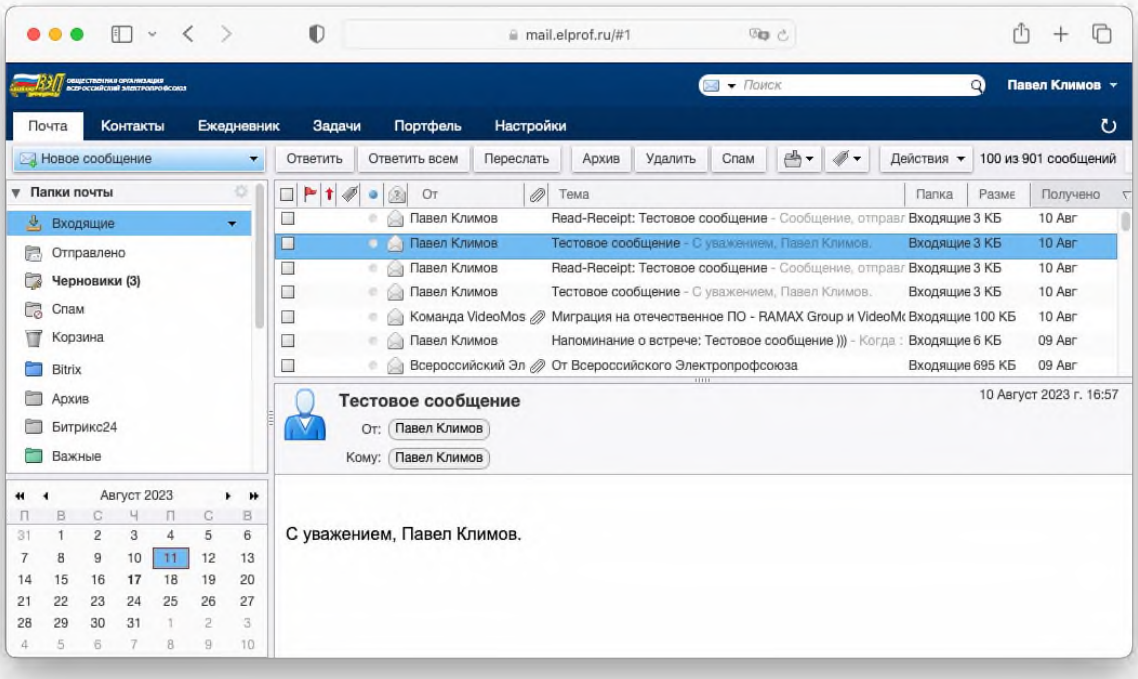


Рисунок № 2

В программный пакет входит стандартный набор приложений, необходимых для любой системы коллективной работы – Почта, Контакты, Ежедневник, Задачи, Портфель.



Открытое рабочее окно почтовой программы. В левом верхнем углу расположен логотип и наименования организации.

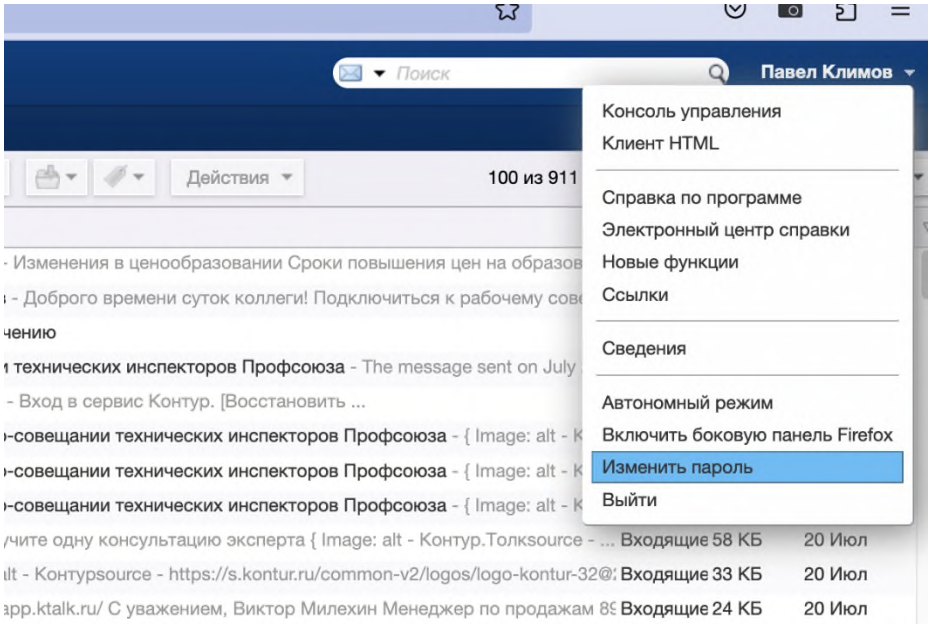
Каждой территориальной организации присвоен общий почтовый ящик следующего формата - reg77@elprof.ru, где reg - буквенное сокращение от английского слова region (регион), 77 - номер региона, в данном примере это Москва. Рассылка будет вестись именно на данные почтовые ящики. К этому почтовому ящику подключаются почтовые ящики председателей территориальных организаций и ответственный за работу с корпоративной почтой со-

трудник. Количество подключаемых сотрудников неограниченно. Для создания ящика сотрудникам необходимо направить письмо-заявку на почтовый ящик - admin@elprof.ru (**имя почтового ящика является псевдонимом, и с данного ящика НИКАКИХ рассылок не производится**) с указанием ФИО сотрудника и занимаемой должности, с созданного ящика председателя территориальной организации.

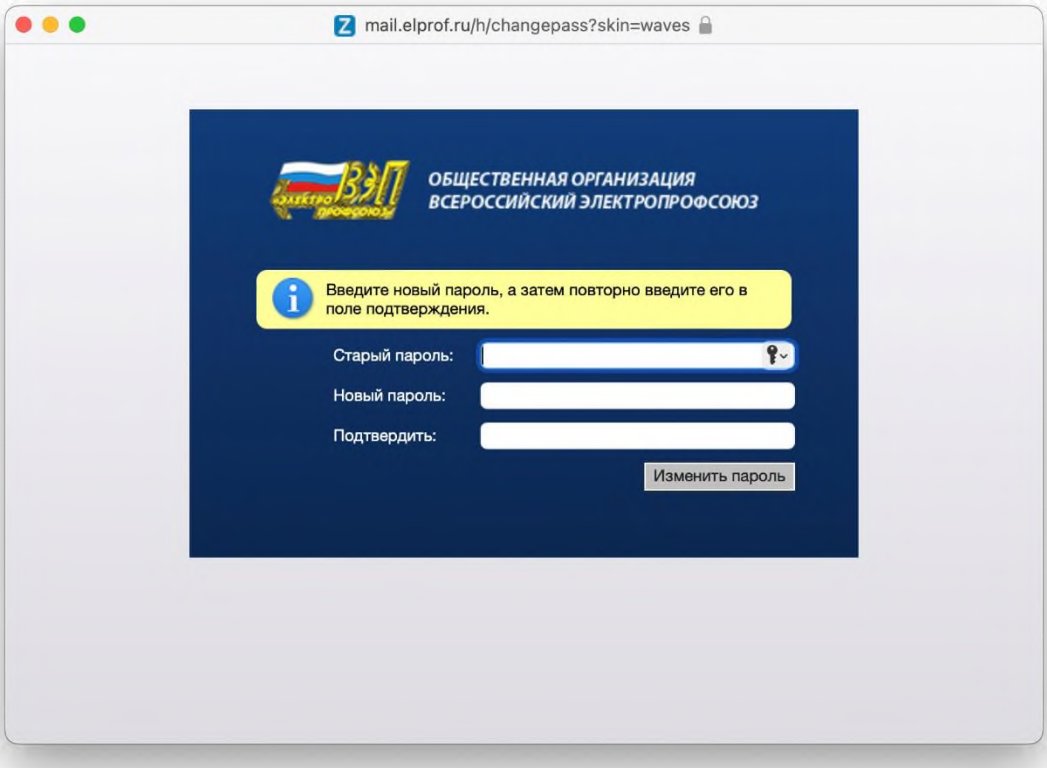
Сотрудникам присвоены почтовые ящики следующего формата - pavel.a.klimov@elprof.ru, **pavel** - имя, **a** - начальная буква отчества, **klimov** - фамилия в транслите (Трансли́т (название произведено сокращением слова «транслитерация») — передача текста с помощью чужого алфавита.) буквами английского алфавита. Сложное название почтового ящика предотвращает подбор имен спамерами.

Смена пароля рекомендована раз в полгода, в целях безопасности можно менять чаще, минимальная длина пароля в сегодняшних реалиях рекомендована от 20 символов, включая строчные и прописные символы, цифры и специальные символы, на пример - **Vco1FN8Mu{gG*?%K** , такой пароль является уникальным и сложен к подбору.

Для того, чтобы сменит пароль, необходимо, в правом верхнем углу нажать на ФИО пользователя и в диалоговом окне выбрать пункт меню – «Изменить пароль»



Далее откроется в новом окне браузера форма для смены пароля, в котором указывается старый пароль, новый и подтверждение нового пароля.



После нажатия на кнопку «Изменить пароль» изменение вступят в силу, в следующий раз, при авторизации старый пароль уже перестанет действовать. Данное окно так же брендировано логотипом и названием организации.

Символов в пароле должно быть не менее двадцати, а лучше больше. Вам не обязательно использовать в пароле все четыре варианта (прописные и строчные буквы, цифры, символы), но в целях повышения безопасности желательно. Два или три из этих варианта достаточно, **но при создании нового пароля не копируйте старый**. Многие люди испытывают сложности при запоминании пароля. Создайте один длинный пароль, который вы запомните. Остальные сохраните в менеджере паролей, например, LastPass, Password Safe или сохраните в тестовом файле на рабочем столе, если Вы уверены в безопасности вашей системы!!!

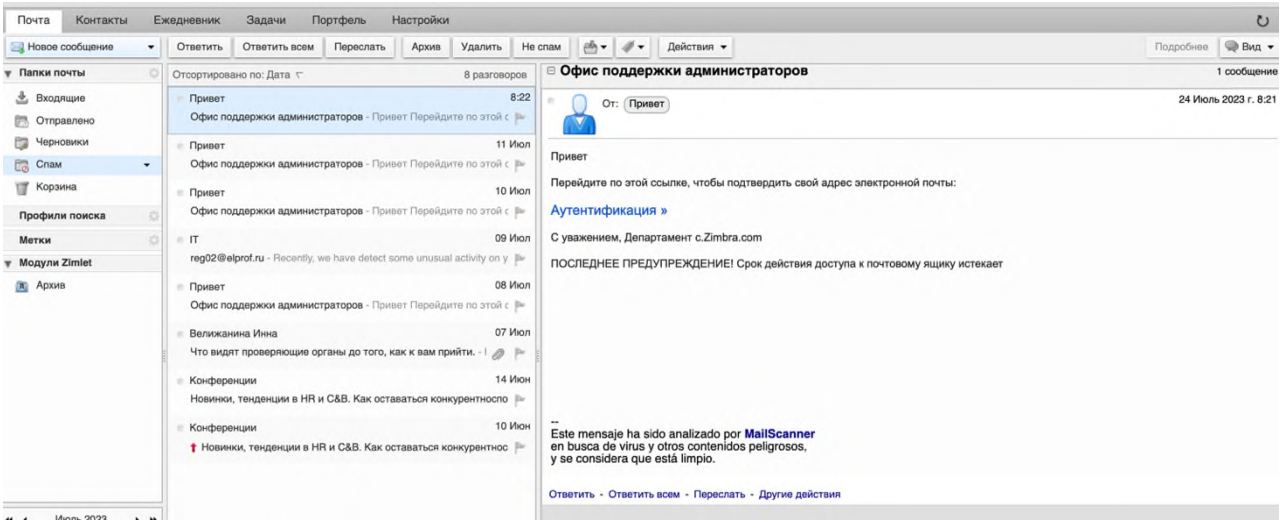
Важно запомнить, что все почтовые ящики не ограничены по объему, но есть ограничения по размеру пересылаемой информации в одном письме, не более **31Мб** данных за одну отправку. Аккаунт пользователя неограничен по длительности использования, то есть администратор не ставит срок действия аккаунта, у самого аккаунта есть 2 статуса – «Активен», либо «Отключен», **и соответственно ни каких ПИСЕМ об окончании срока действия аккаунта, о том, что закончилось место, Ваша учетная запись заблокирована и нужно подтвердить ее при помощи введения логина и пароля, ни Администратор Zimbra, ни Администратор домена, ни другие вымышленные персонажи, а так же человек, который в действительности ответственен за работу Системы обмена документами на базе программного обеспечения Zimbra, НЕ ОТПРАВЛЯЕТ!!!**

Получение данных об аккаунтах пользователей называется «фишинг», то есть в переводе на русский – рыбалка. Злоумышленник закидывает «наживку», связанную с аккаунтом пользователя, и пытается обманным пу-

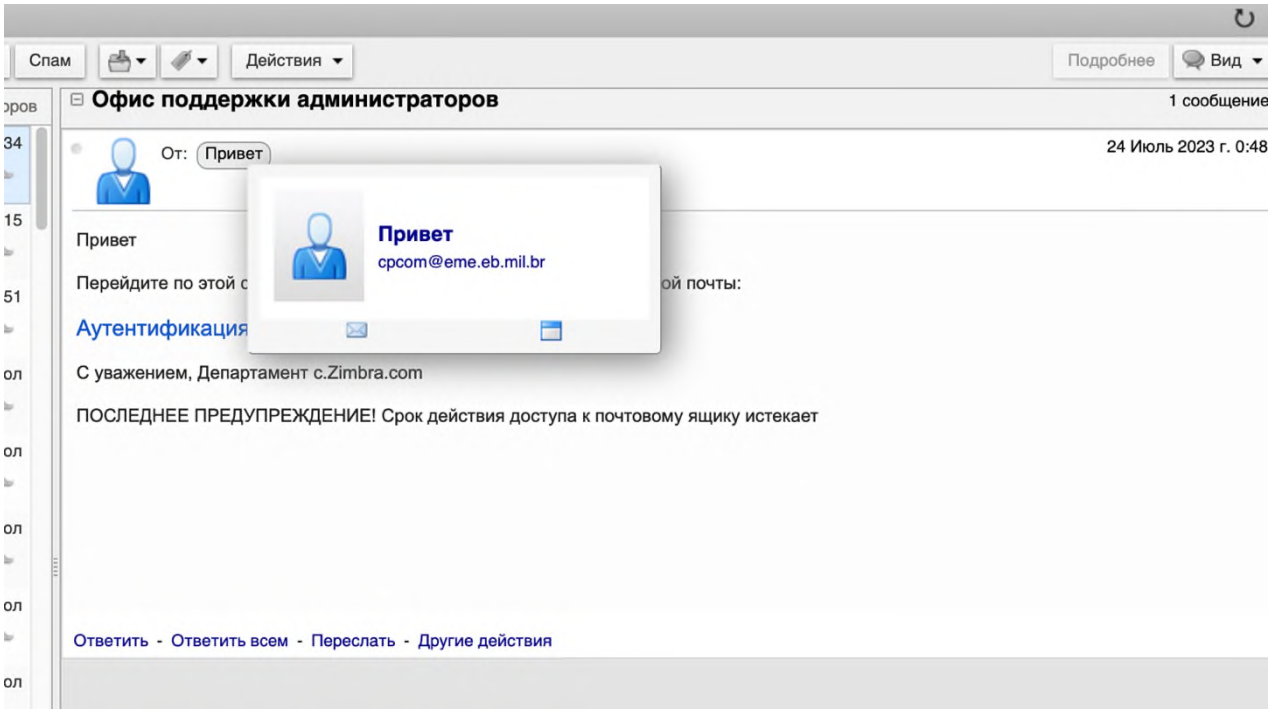
тем получить данные от почтового «ящика». Целью, как правило, является рассылка спама!

Типы фишинговых атак

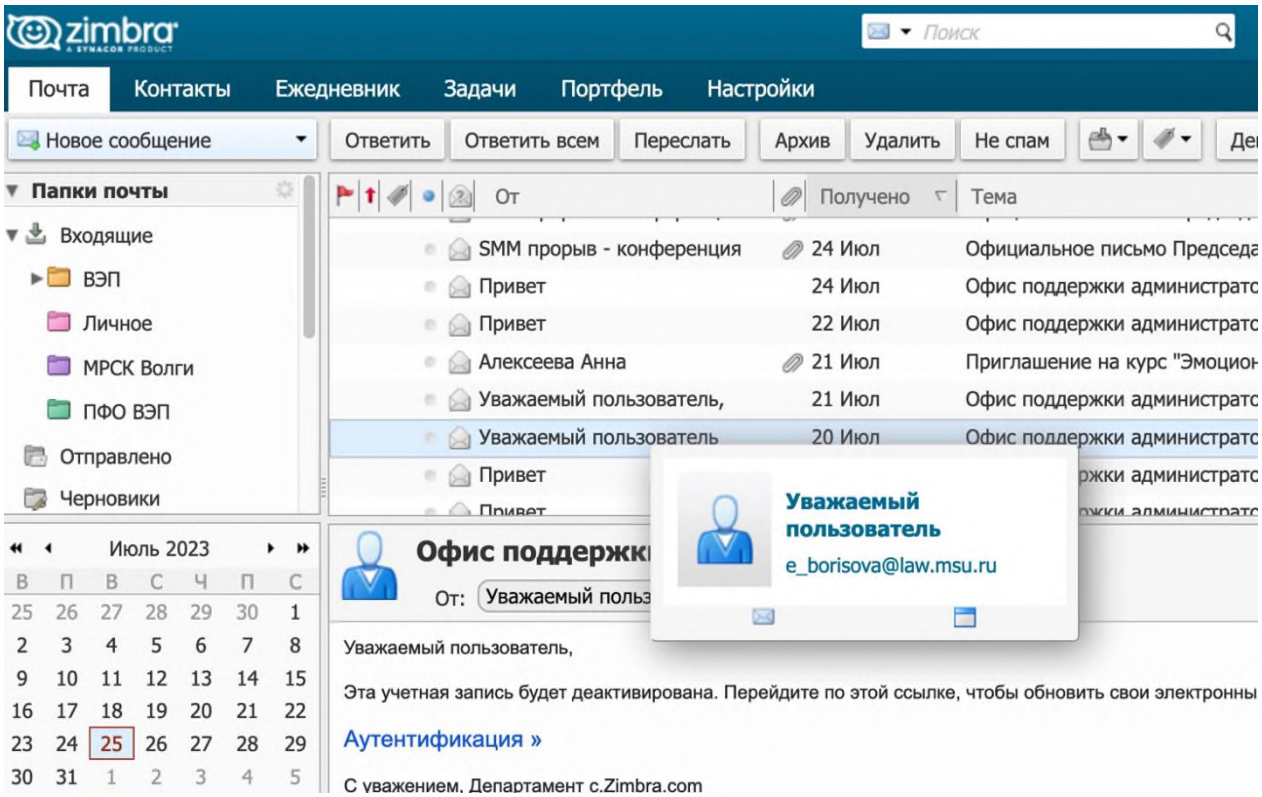
- **Фишинг через электронную почту — злоумышленник посылает электронное письмо, которым намеревается вас встревожить или заинтриговать. Ему нужно, чтобы вы нажали на ссылку, указанную в письме**.
- При вишинге злоумышленник звонит на стационарный, мобильный или VoIP-телефон, чтобы вовлечь пользователя в разговор.
- Смишинг — преступник присылает СМС с просьбой нажать на ссылку или позвонить отправителю.
- Фарминг — так как все больше людей узнают, что опасно переходить по ссылке в нежданном электронном письме, злоумышленники создали фарминг. Фарминг-атака включает в себя вредоносный URL-адрес, в надежде, что вы его скопируете, вставите в свой браузер и получите доступ к веб-сайту. Фарминг компрометирует локальный кэш DNS, который в результате будет направлять вас на поддельные сайты вместо реальных. Вредоносная ссылка приведет вас на поддельный веб-сайт.
- **Направленный фишинг — злоумышленник присылает электронные письма, нацеленные на конкретную организацию или группу лиц. Направленные фишинговые письма обычно адресуются руководителям или сотрудникам финансовых отделов.**
- Уэйлинг похож на направленный фишинг, но целью уэйлинга являются руководители высшего звена.



Сообщение при попытке «фишинга»

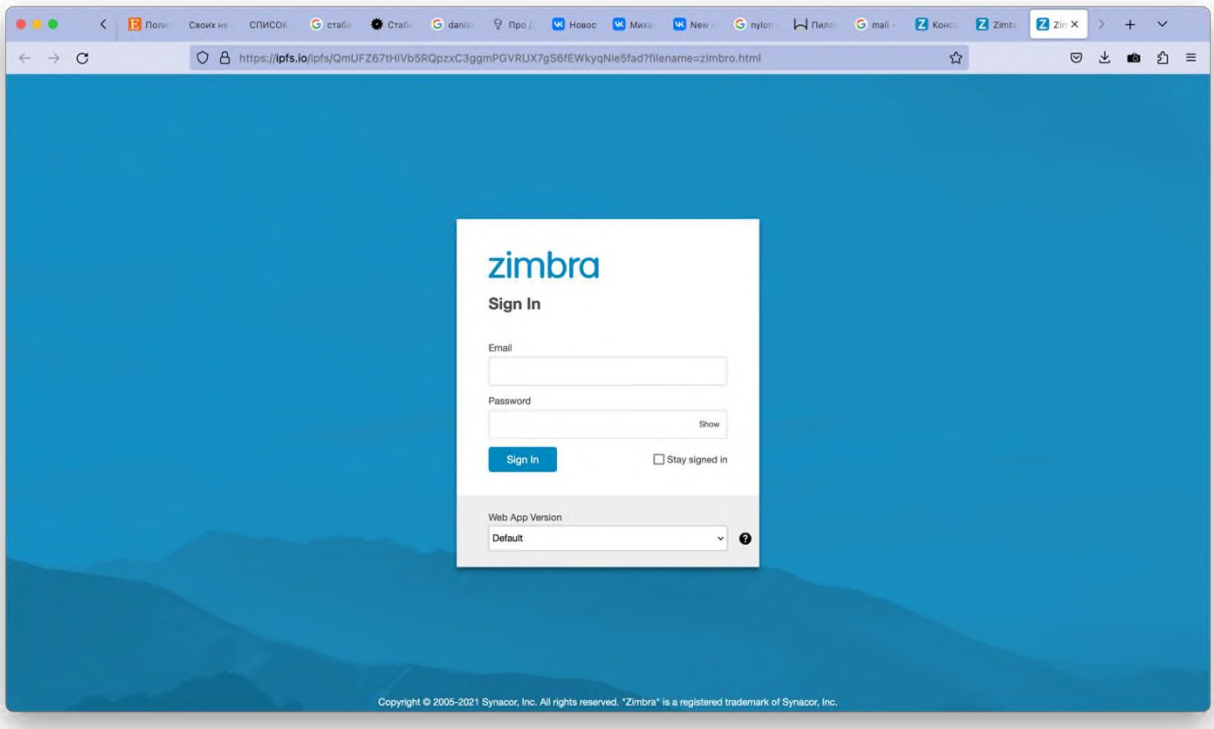


Сообщение при попытке «фишинга»



Еще вариант фишингового сообщения и снова тема – «Офис поддержки администраторов», на примере отчета о фишинговых атаках на почтовые ящики, который представлен ниже, сообщения такого характера на русском языке (кириллице) будут выглядеть так:

From =?UTF-8?B?0KDQtdC00LDQutGG0LjRjyDQs9Cw0LfQtdGC0Ys=?= =?...

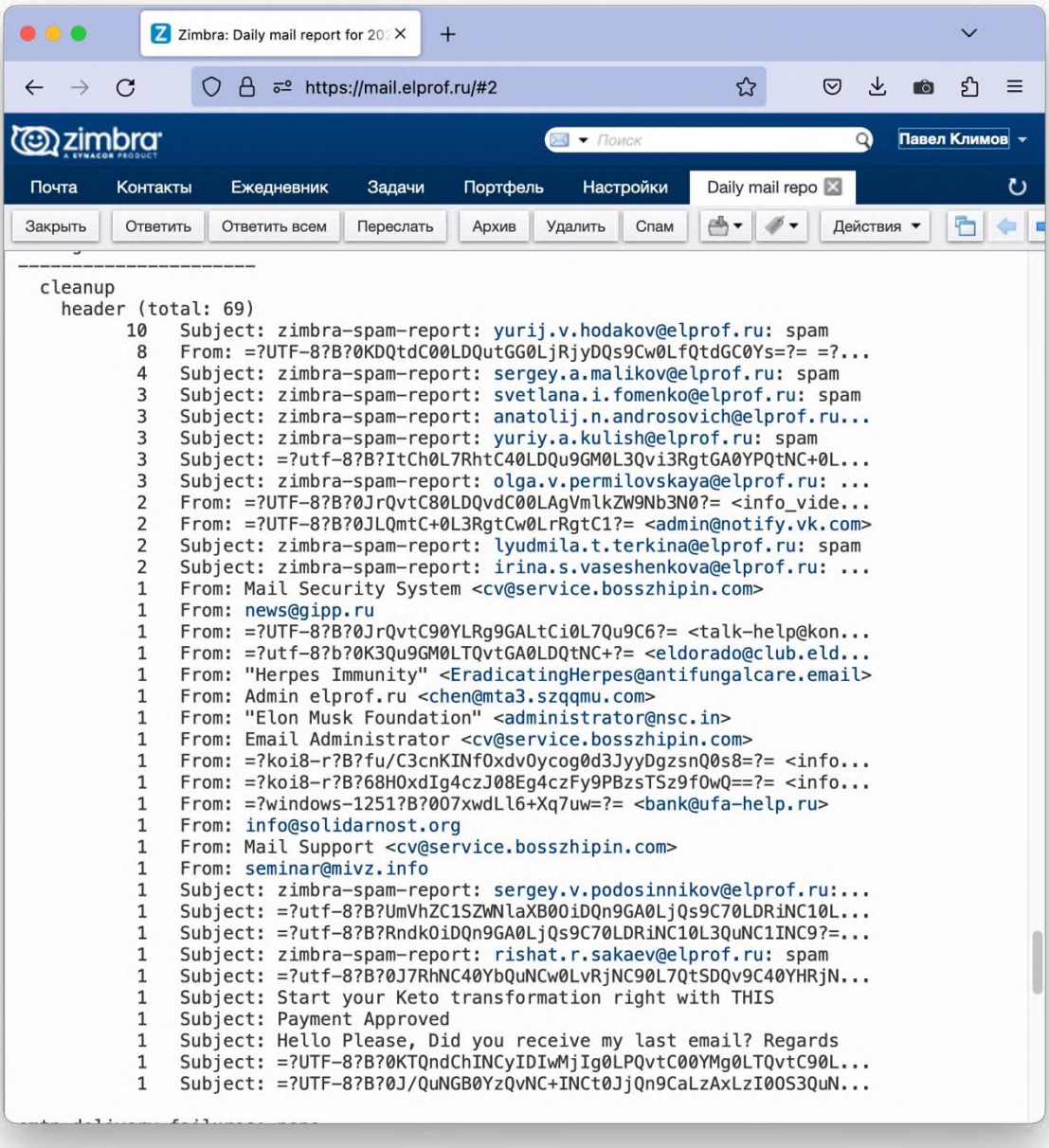


Вот так выглядит страница, при переходе по ссылке, указанной в письме как на примере, показанном выше, ничего общего со страницей входа в почтовую программу ВЭП, тем более, название сайта в адресной строке браузера кардинально отличается от адреса **https://mail.elprof.ru**

Есть много способов защититься от «фишинга». Первое и самое важное – соблюдать осторожность и следовать следующим незамысловатым правилам:

- **Внимательно изучите электронное письмо, прежде чем нажать на ссылку. Наведите указатель мыши на адрес отправителя письма и на ссылку. Это может раскрыть информацию, указывающую на то, что письмо фишинговое.**
- **Перед вводом конфиденциальных данных на сайте внимательно проверяйте URL-адрес страницы. Настоящий ли это вебсайт? Не содержит ли его адрес лишних букв? Не заменены ли буквы цифрами (например, буква О на ноль)? Бывает трудно заметить различия.**
- **Прежде чем переходить по ссылкам из постов, размещенных от имени ваших друзей, подумайте. То, что выглядит слишком хорошо, чтобы быть правдой, чаще всего оказывается ложью.**

Для предотвращения «фишинга» работает анализ заголовков самих сообщений. В систему занесены одни из самых распространённых тем писем, заголовков «от кого».



Ежесуточный отчет о фишинговых письмах

Как видно из отчета, в списке присутствуют письма от имени администратора, на пример - **From: Admin elprof.ru chen@mta3.szqqmu.com** в поле от «Кого» (From) стоит название доменного имени официального сайта ВЭП, но дальше идет адрес отправителя и после @ доменное имя кардинально отличается от официального доменного имения сайта ВЭП.

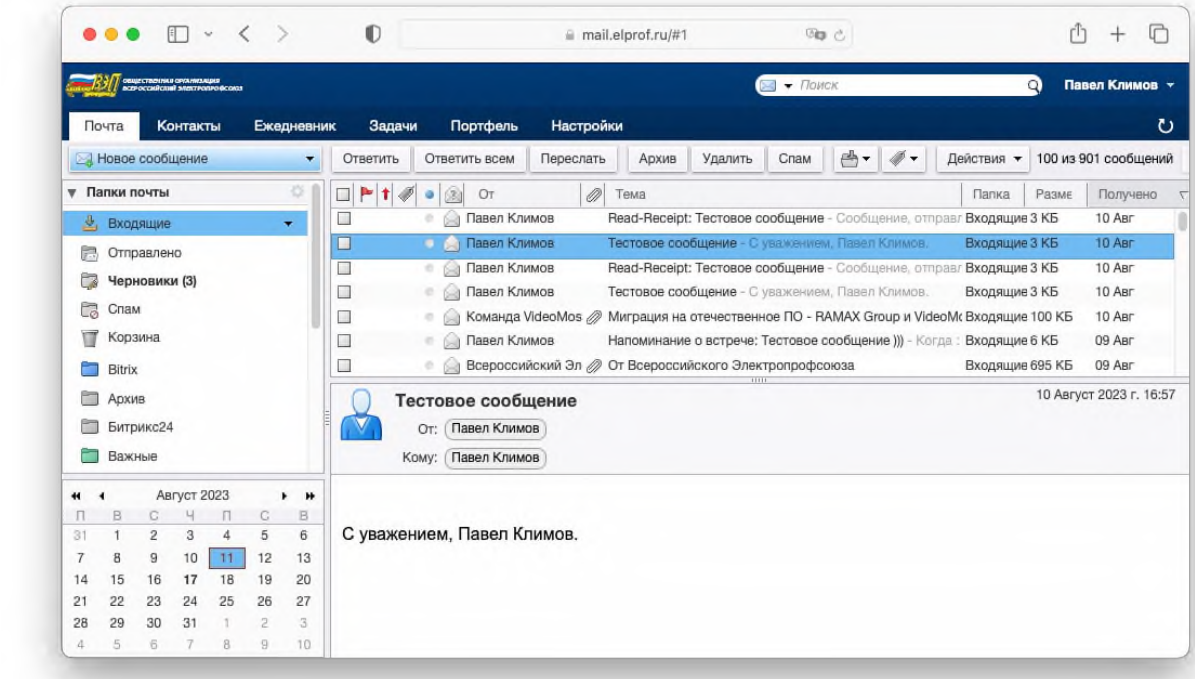
From: Mail Security System cv@service.bosszhipin.com, From: Email Administrator cv@service.bosszhipin.com, From: Mail Support cv@service.bosszhipin.com, Subject: Hello Please, Did you receive my last email? Regards – все эти сообщения заблокированные системой распознавания фишинговых атак по заголовкам письма. Система распознавания может так же анализировать фрагменты текста.

Выше представлен ежедневный отчет системы блокировки попыток подбора пароля к пользователям, в пиковые нагрузки работы сервера число попыток может доходить до десятков тысяч за сутки.

SASL PLAIN authentication failed - это сообщение означает, что попытка войти в тот или иной аккаунт пользователя с паролем закончилась неудачей. Такие попытки атак на аккаунты пользователя происходят ежесекундно. Система анализа Fail2Ban блокирует неизвестные IP адреса по следующему алгоритму. Первые три попытки авторизоваться она пропускает, так как пользователь действительно мог забыть пароль, после третий неудачной попытки IP адрес блокируется на 5 минут, если с данного IP продолжаются попытки ввести пароль, то система блокирует на 30 минут, если в течении суток попытки войти продолжаются, то в таком случае система блокирует IP адрес на 72 часа. Минус данной системы заключается в том, что злоумышленник может находится на одном и том же IP адресе, что и пользователь, и

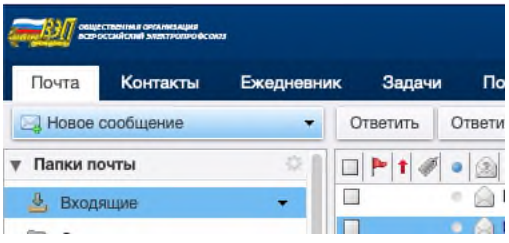
пользователь может быть заблокирован по ошибке. На данный случай предусмотрена дополнительная проверка – IP пользователя будет исключен из «черного списка» через 72 часа и если с данного адреса снова поступают попытки подобрать пароль, то в этом случае IP блокируется на неопределенный срок.

В любом браузере (программа для работы в Internet – рисунок № 1) в адресной строке необходимо ввести адрес почтового сервера **https://mail.elprof.ru.** После авторизации вы попадаете на главную страницу почтовой программы.

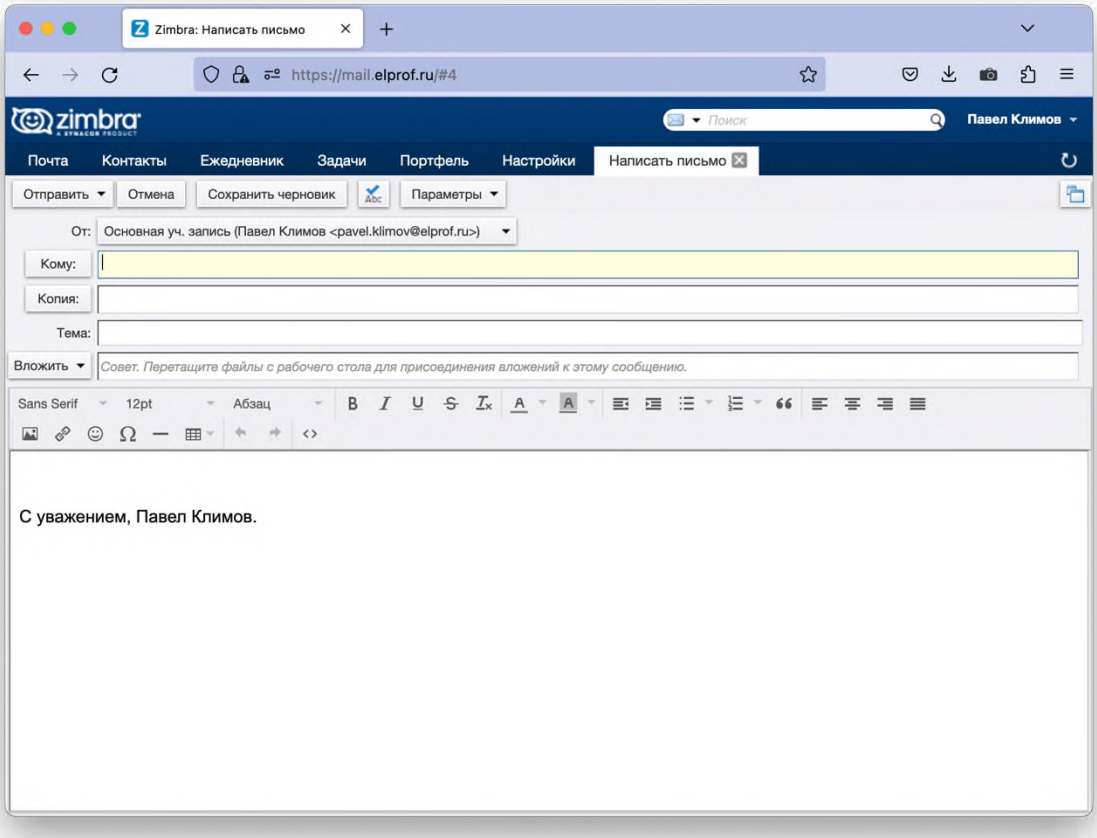


Интерфейс во многом напоминает любой почтовый клиент, таких как Mail.ru, Yandex Mail, GMAIL.

Для того, чтобы написать письмо, необходимо выбрать в вкладке «Почта» - «Новое сообщение».

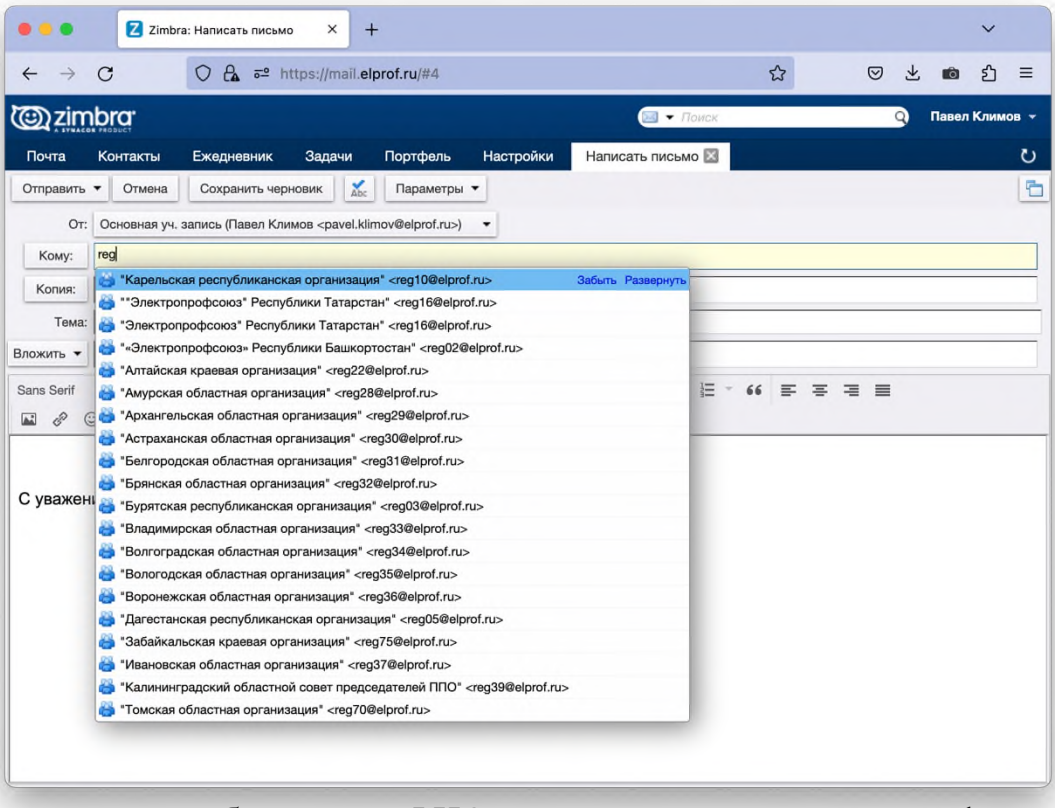


Далее откроется вкладка программы «Написать письмо», с полями «Кому». В данное поле вводится адрес получателя. В поле «Копия» вводится адрес получателя для отправки копии сообщения, если это необходимо отправителю. Поле «Тема» служит для удобства поиска отправленных или входящих писем и обязательно к заполнению. Поле «Вложить» позволяет прикрепить файл(ы) для отправки вместе с сообщением, при этом объем пересылаемого сообщения не должен превышать 31МБ!

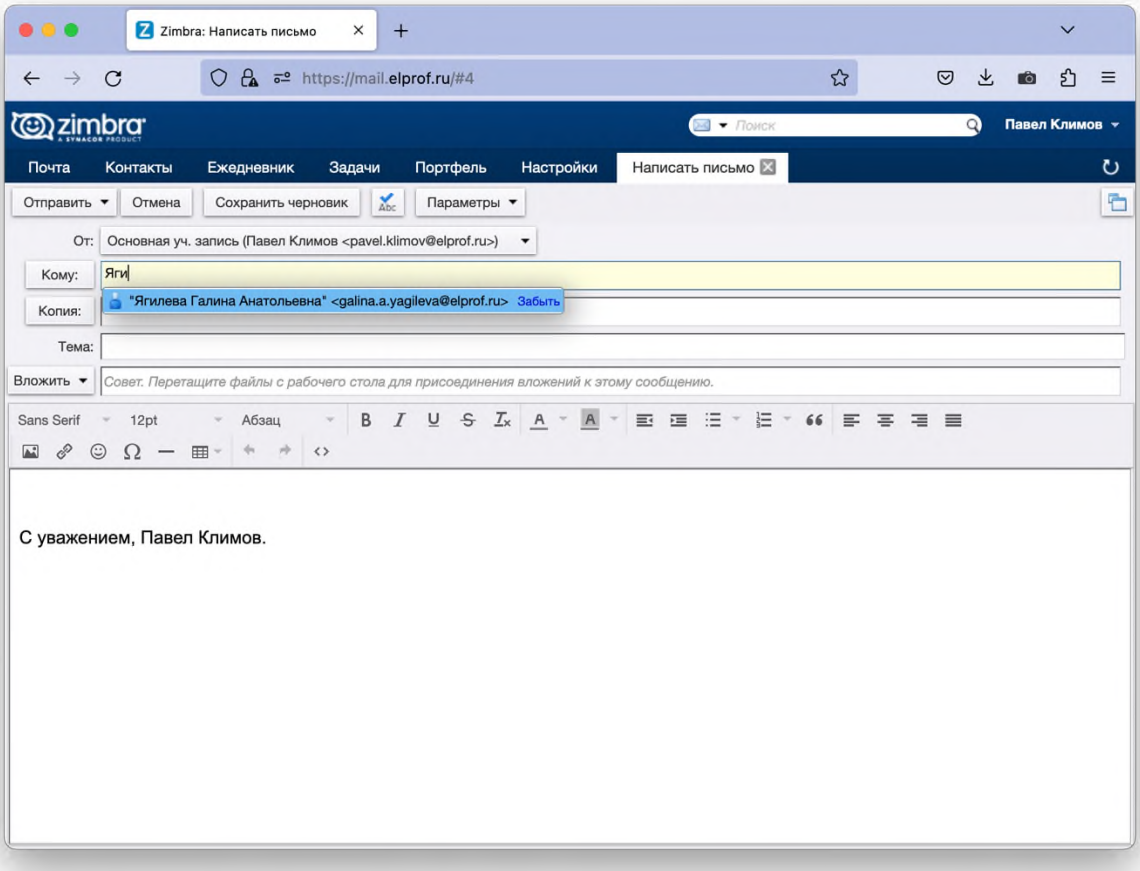


Для отправки письма в какую-либо территориальную организацию ВЭП необходимо выбрать во вкладке «Почта» – «Новое сообщение» и набрать номер или название региона. Региональные ящики начинаются на reg**@elprof.ru.

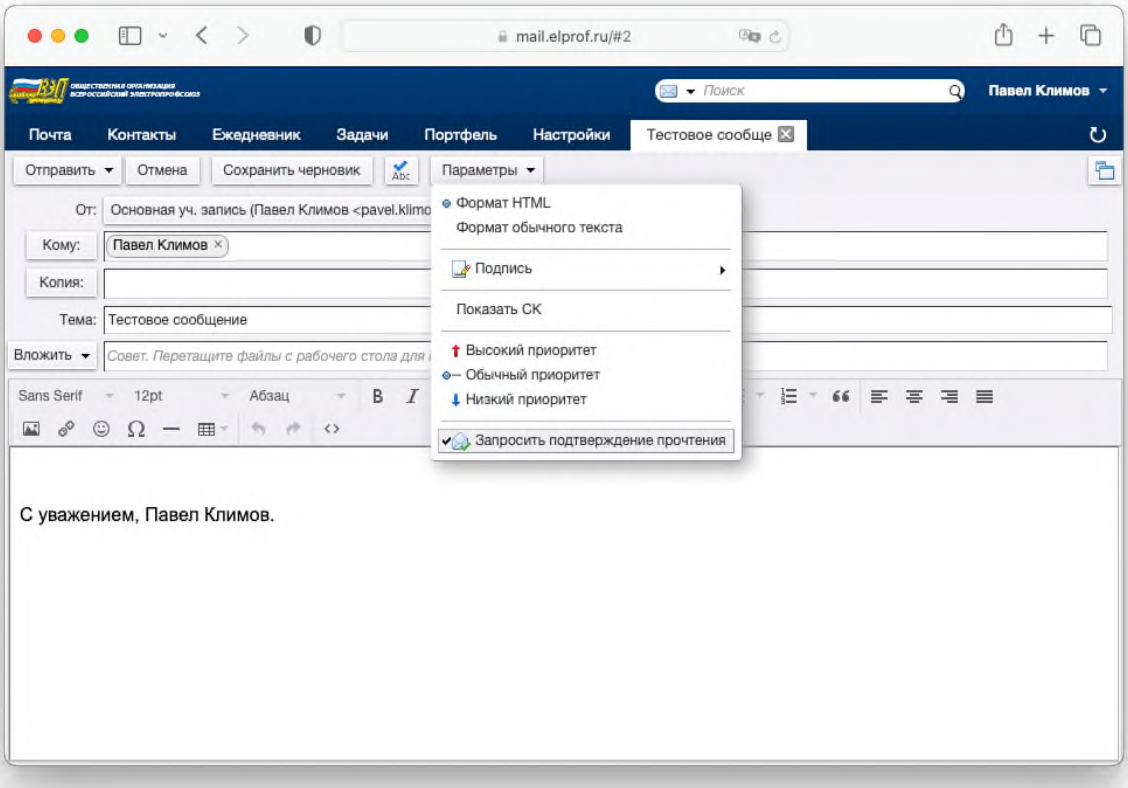
Для массовой рассылки в поле «Кому» надо набрать слово «Всем» – письмо будет отправлено всем территориальным организациям ВЭП.



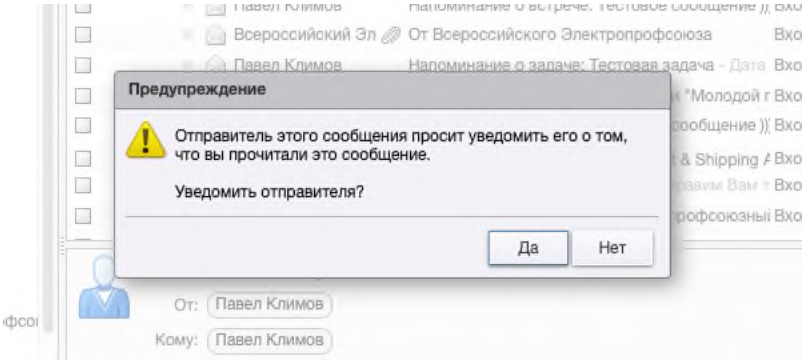
Для отправки сообщения по ФИО достаточно начать печатать фамилию адресата, как показано на рисунке ниже.



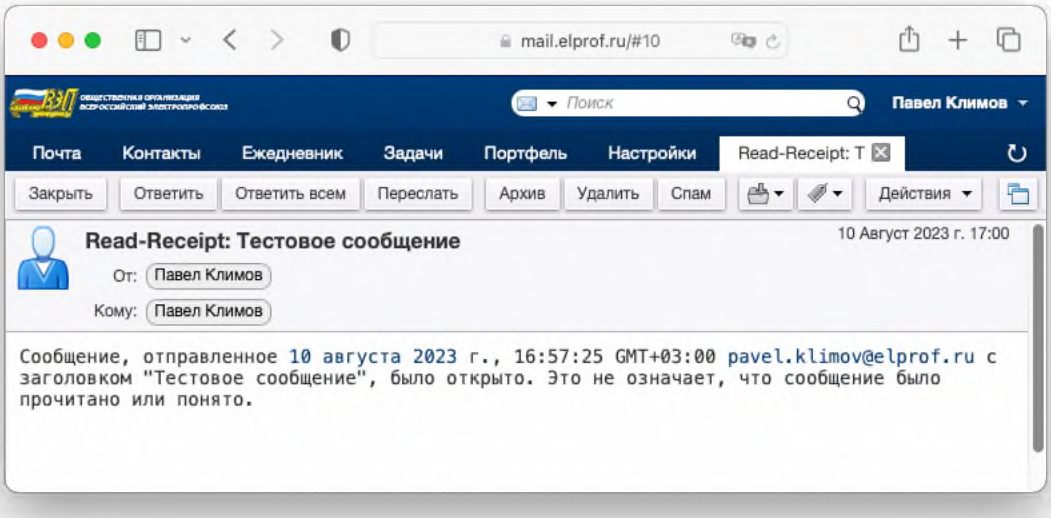
Для отправки сообщения с последующим уведомлением о прочтении сообщения необходимо перед отправкой включить «Параметры» – «Запросить подтверждение отправки».



При получении письма появится диалоговое окно с предупреждением, что на это сообщение отправитель запрашивает уведомление о получении письма.

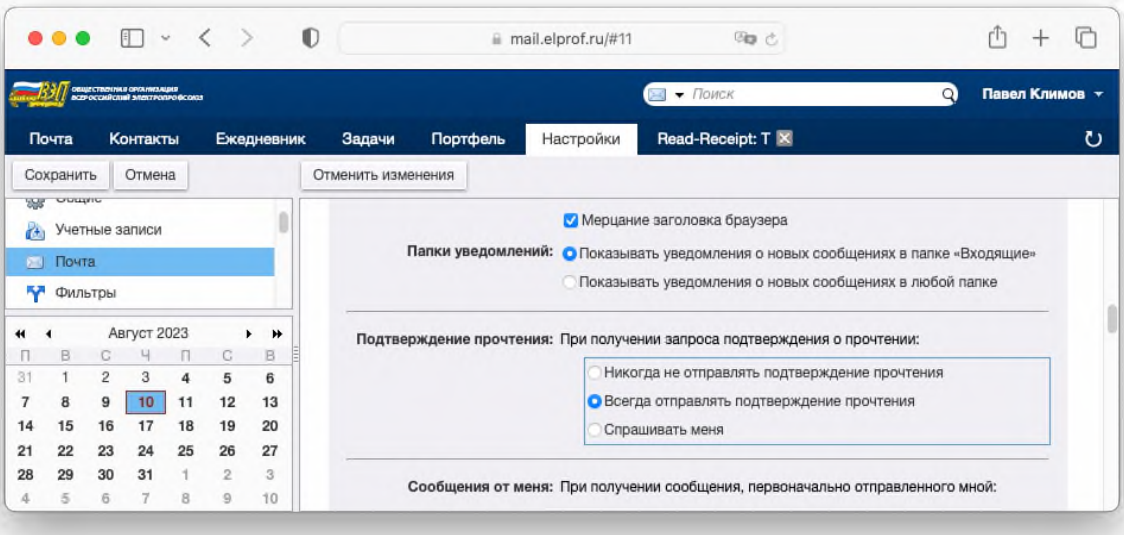


Если подтвердить отправку отчета о доставке нажать «ДА», то отправителю придет следующего вида сообщение:

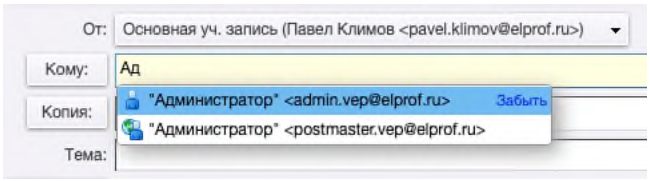


В случае отрицательного ответа отправитель не получит никакой обратной связи.

Также во вкладке «Настройки» в подразделе «Почта» можно настроить автоматическое получение подтверждений о прочтении сообщений.



ТЕХНИЧЕСКАЯ ПОДДЕРЖКА



Любые вопросы по работе Системы обмена документами на основе программного продукта можно направлять на электронный ящик admin@elprof.ru, хочу обратить внимание, данный ящик служит только для приема обращений от пользователей и с данного ящика никаких уведомлений и рассылок не производится. Все информационные рассылки о работе системы производятся с ящика

"Павел Климов" <pavel.klimov@elprof.ru>

Так же можно обращаться в WhatsApp по номеру +7 (915) 041-43-27

ПРИМЕЧАНИЯ!

- В инструкции использованы скриншоты (снимки экрана), на которых отсутствует логотип и названия организации в качестве демонстрации возможностей системы.
- Скриншот (снимок экрана) может отличатся по внешнему виду окном браузера из-за разницы используемой операционной системы и используемого браузера.