ЕВРОАЗИАТСКИЙ
РЕГИСТРАТОР

РЕКОМЕНДАЦИИ КЛИЕНТАМ

по соблюдению мер информационной безопасности при использовании информационных сервисов ООО «Евроазиатский Регистратор»

Во избежание инцидентов, связанных с неправомерным использованием Вашей компьютерной техники, используемой для работы с информационными сервисами ООО «Евроазиатский Регистратор»», убедительно просим Вас неукоснительно соблюдать рекомендуемые правила безопасности.

Только комплексное соблюдение описанных правил безопасности позволит Вам не стать жертвой мошенников и иных злоумышленников и поможет обеспечить защиту ВАШИХ ДАННЫХ.

1. Рекомендации по защите информации от воздействия вредоносного кода

1.1. На персональном компьютере Клиента должно быть установлено лицензированное антивирусное программное обеспечение (ПО). Антивирусное ПО должно регулярно обновляться. Рекомендуется установить по умолчанию максимальный уровень политики безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов производится антивирусным ПО в автоматическом режиме.

1.2. Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного ПО.

1.3. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т.п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.

1.4. При использовании сети Интернет для обмена почтовыми сообщениями необходимо применять антивирусное ПО, поддерживающее проверку почтовых клиентов.

1.5. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа ПО, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т.п.) или нарушения работоспособности компьютера необходимо осуществить внеплановую проверку на наличие вредоносного ПО. После удаления вирусов и восстановления работоспособности компьютера необходимо произвести смену паролей на новые, удовлетворяющие требованиям п. 3.1 .

1.6. Не открывайте файлы, полученные по электронной почте от неизвестных отправителей.

1.7. Не используйте незащищенные ресурсы, такие как HTTP. В случае предупреждений вашего браузера о небезопасном соединении, никогда не вводите логины и пароли, закройте такой сайт.

2. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

2.1. Мошеннический или поддельный web-сайт - это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете (например, банка), и предназначены для сбора конфиденциальной информации обманным путем.

2.2. Вход в информационный сервис «Личный кабинет Акционера» необходимо осуществлять только с сайта **https://lk.earc.ru**. Вход в информационный сервис «Личный кабинет Эмитента» необходимо осуществлять только с сайта **https://lke.earc.ru.** Обращайте внимание, что в адресной строке браузера присутствует именно этот адрес, остерегайтесь похожих названий. Не вводите аутентификационных данных на любых других сайтах.

2.3. Перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании. Изменить адрес электронной почты отправителя очень просто, поэтому будьте бдительны.

2.4. Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это - электронное письмо, отправленное мошенниками.

2.5. Старайтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить Вас в том, что Вашему счету угрожает опасность, если Вы немедленно не обновите критически важные данные.

2.6. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не переходите по этой ссылке.

2.7. Не устанавливайте программное обеспечение, которое рекомендуют такие письма.

2.8. Не переходите по ссылкам в таких письмах. При необходимости наберите адрес ссылки из письма в программе «Блокнот» и скопируйте в браузер уже из приложения «Блокнот».

3. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

3.1. Рекомендуется регулярно менять пароли для работы со своими учетными данными в различных системах. Длина Вашего пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

3.2. Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные (например, портал Госуслуг, онлайн-Банкинг и т. д.).

3.3. В случае компрометации или подозрениях на компрометацию пароля, рекомендуется незамедлительно сменить пароль на новый, удовлетворяющий требованиям п. 3.1 .

3.4. Никому передавайте и не разглашайте свои пароли. Если кто-то просит вас сказать ваш пароль, то скорее всего это мошенники.

3.5. Рекомендуется установить пароли на учётные записи пользователей операционной системы на компьютере.

3.6. Рекомендуется исключить возможность физического доступа посторонних лиц к компьютеру, с которого Вы осуществляете работу.

3.7. Блокируйте экран, чтобы посторонние лица не смогли воспользоваться вашими учетными данными.

3.8. Рекомендуется применять на компьютере для работы специализированные программные и аппаратные средства безопасности: средства защиты от несанкционированного доступа, персональные межсетевые экраны, антишпионское программное обеспечение и т.п., обеспечить регулярное автоматическое обновление программного обеспечения этих средств.

3.9. На компьютере для работы необходимо исключить посещение WEB-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т.п. Использование нелицензионного программного обеспечения повышает риск получения несанкционированного доступа злоумышленников с целью хищения информации.

3.10. Включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ; старайтесь периодически просматривать журнал и реагировать на ошибки.

3.11. При работе в общественных местах не допускайте, чтобы экран вашего устройства находился в зоне видимости посторонних лиц.

3.12. Мы не рекомендуем вам подключаться к Интернет через общедоступные Wi-Fi точки доступа. В качестве альтернативного способа используйте телефон и мобильную передачу данных. Чтобы избежать автоматического подключения к Wi-Fi, настройте функцию Wi-Fi подключения выключенной по умолчанию.