Утверждено
Приказом Генерального Директора
ООО «ИК «Грандис Капитал»
№ Р-05-007/2019 от «31» мая 2019 г.

Вводится в действие с «31» мая 2019 года.

# РЕКОМЕНДАЦИИ КЛИЕНТАМ ООО «ИК «Грандис Капитал»

## по обеспечению защиты информации, в т.ч. в целях противодействия осуществлению незаконных финансовых операций.

### 1. Общие положения

1.1. Настоящие рекомендации предназначены для клиентов ООО «ИК «Грандис Капитал» (далее – Компания) в целях защиты информации и предотвращения осуществления незаконных финансовых операций.

1.2. Задачи защиты информации сводятся к минимизации ущерба и предотвращению воздействий со стороны злоумышленников. Для обеспечения надлежащей степени защищенности должен быть обеспечен комплексный подход, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне Компании, так и на стороне клиента.

1.3. Наиболее опасным является кража учетных данных - хищение личных данных клиента Компании и их незаконное использование для выполнения несанкционированных операций от имени клиента. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций.

1.4. Риски получения несанкционированного доступа к информации прежде всего связаны с «фишингом» (использованием ложных ресурсов сети Интернет с целью получения доступа к распоряжению денежными средствами и ценными бумагами лицами, не обладающими такими правами), а также воздействием вредоносного кода.

1.5. «Фишинг» - попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

1.6. Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах, с которых осуществляется работа с системой, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее - ПО) либо на перехват информации, в том числе паролей.

1.7. Средства и методы защиты информации, применяемые в Компании, позволяют обеспечить необходимый уровень безопасности при осуществлении финансовых операций и иных операций и предотвратить мошеннический действия, направленные на несанкционированный доступ к распоряжению денежными средствами и ценными бумагами клиентов при условии выполнения клиентами рекомендаций, изложенных в данном документе.

### 2. Рекомендации по защите информации от воздействия вредоносного кода.

2.1. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от

неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

2.2. Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.

2.3. Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).

2.4. Не используйте права администратора при отсутствии необходимости; в повседневной практике входите в систему с учетной записью пользователя, не имеющего прав администратора.

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

2.6. Не используйте на устройстве, предназначенного для доступа к Системе Брокерского обслуживания TRANSAQ и/или к Системе Электронного документооборота «Брокер-Клиент» (далее Системы ДО), средства удаленного администрирования.

2.7. Обязательно установите и своевременно обновляйте на компьютере антивирусное программное обеспечение. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов производится антивирусным средством в автоматическом режиме.

2.8. 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 средства.

2.9. Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы.

2.10. 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.

2.11. При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам Сети Интернет.

2.12. При работе в Интернет не соглашайтесь на установку каких-либо сомнительных программ.

2.13. Воздерживайтесь от использования программ онлайнового общения на компьютере, использующемся для работы в системах Компании по дистанционному обслуживанию.

2.14. Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ.

2.15. Рекомендуем ограничить информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты. Старайтесь не использовать компьютер, с которого Вы осуществляете переводы денежных средств, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

2.16. Важно знать, что надежным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто в виде «интересной ссылки» в письме от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.

2.17. При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), полностью воздержаться от использования систем дистанционного обслуживания в Компании и проведения финансовых и иных операций до исправления ситуации.

2.18. **Помните**, что Компания не несет ответственности в случае возникновения финансовых потерь, понесенных Клиентом в связи с нарушением и/или ненадлежащим исполнением им требований по защите от вредоносного кода своих автоматизированных рабочих мест (компьютера, ноутбука) для доступа к Системам ДО.

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

3.1. 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, Компании), и предназначены для сбора конфиденциальной информации обманным путем.

3.2. Злоумышленниками возможно создание фальсифицированных WEB-сайтов - их доменные имена и стили оформления могут имитировать сайты Компании и содержать ложные реквизиты и контактную информацию. Вступление в какие- либо деловые отношения с лицами, представляющими ложный ресурс и использование подобных реквизитов, рискованно и может привести к нежелательным последствиям. Ввод логина и пароля на таком сайте приводит к получению этих данных злоумышленниками, т.е. разглашению идентификационных данных. Помните, что сайты, визуально напоминающие сайт Систем ДБ, создаются специально для незаконного получения информации. В случае обнаружения фальсифицированного сайта, копирующего дизайн официального сайта Системы ДО, пожалуйста, незамедлительно сообщите об этом по контактным телефонам Компании.

3.3. Во избежание использования ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемой Компанией в Системе ДО, и (или) использующих зарегистрированные товарные знаки и наименование Компании, необходимо удостовериться, чтобы при подключении к Системам ДО защищённое SSL-соединение было установлено исключительно с официальным сайтом Системы ДО. Прежде чем ввести логин и пароль, Клиентам необходимо проверить по информации из SSL-сертификата подлинность сайта.

3.4. 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.

3.5. 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.

3.6. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. В настоящем электронном письме Компания всегда приветствует Вас, обращаясь по имени и фамилии либо по названию компании. Типичное фишинговое письмо начинается с обезличенного приветствия.

3.7. 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.

3.8. 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.

## 4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

4.1. Рекомендуется выделить отдельный компьютер, который использовать только для работы в Системами ДО.

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

4.3. Используемые в Системах ДО логины и пароли, запрещается записывать и хранить в местах, доступных посторонним лицам.

4.4. Необходимо хранить пароль в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования. Не рекомендуется записывать логин и пароль к Системам ДО там, где доступ к нему могут получить посторонние лица;

4.5. Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, на которых Вы вводите конфиденциальные данные.

4.6. В том случае, если Вы обнаружили, что Ваш пароль от Системы ДО скомпрометирован, рекомендуем Вам незамедлительно сменить пароль на новый, известный только Вам, удовлетворяющий требованиям п. 4.2.

4.7. Если в процессе работы Вы столкнулись с тем, что ранее действующий пароль не срабатывает и не позволяет Вам войти в систему, необходимо как можно быстрее обратиться в Компанию для получения инструкций по смене пароля.

4.8. Никому не разглашайте пароль от Систем ДО. Компания не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные (в т.ч. пароли и т.п.).

4.9. Не пересылайте файлы с конфиденциальной информацией для работы с Системами ДО по электронной почте или через SMS-сообщения.

4.10. Рекомендуем исключить возможность физического доступа к компьютеру, с которого Вы осуществляете работу, не имеющего отношения к работе с Системами ДО и посторонних лиц.

4.11. Незамедлительно обращайтесь в Компанию в том случае, если Вы получили уведомление системы об операции, которую Вы не проводили.

4.12. Размещение, охрана и специальное оборудование помещения, в котором установлены компьютеры, используемые для доступа в систему, должны обеспечивать сохранность информации, исключать возможность неконтролируемого проникновения в это помещение;

4.13. Принять меры по контролю конфигурации компьютера, с использованием которого осуществляется доступ к Системам ДО, и их изменения. Не допускать несанкционированных программно-аппаратных изменений конфигурации;

4.14. На компьютере для работы с Системами ДО необходимо использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечить регулярную своевременную установку обновлений, выпускаемых разработчиками ДБО, операционной системы, web-браузеров (Microsoft Internet Explorer, Mozilla FireFox, Opera и т.д.) и иного прикладного программного обеспечения;

4.15. Применять на компьютере для работы с Системами ДО лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновление компонентов антивирусной защиты;

4.16. Рекомендуется применять на компьютере для работы с Системами ДО 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;

4.17. На компьютере для работы с Системами ДО 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 денежных средств;

4.18. Не допускается работать с Системами ДО на компьютерах в Интернет-кафе или на других компьютерах общего пользования (вокзалы, аэропорты, библиотеки и т.п.). Работа с гостевых рабочих мест увеличивает риск неправомерного использования ключа ЭП и другой аутентификационной информации;

4.19. Рекомендуется установить пароли на учётные записи пользователей операционной системы на компьютере для работы с Системами ДО. Работу с Системами ДО на компьютере осуществлять только под учетной записью с ограниченными правами в операционной системе. Не допускать штатную работу в Системах ДО под учетной записью с правами администратора в операционной системе компьютера;

4.20. В случае компрометации или подозрении на компрометацию закрытого ключа ЭП, для предотвращения несанкционированного доступа к управлению счетом, в том числе при утрате (потере, хищении) Ключевого носителя, с использованием которого Клиент осуществляет перевод денежных средств, Клиенту необходимо незамедлительно обратиться в Компанию для блокирования скомпрометированных ключей ЭП;

4.21. Регулярно контролировать состояние своих счетов и незамедлительно сообщать в Компания обо всех подозрительных или несанкционированных изменениях;

4.22. При обслуживании компьютера сотрудниками технической поддержки организации Клиента или сторонних организаций - обеспечивать контроль выполняемых ими действий;

4.23. В случае передачи (списания) компьютера, на котором ранее была установлена Система ДО, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу организации Клиента, в том числе следы работы в Системах ДО;

4.24. Необходимо корректно завершать работу в Системе ДО, используя для этого пункт меню «Выйти из системы».