

Приложение № 1
к приказу
ООО «Клиника
гормонального здоровья»

от 04 декабря 2024 № 18

ПРАВИЛА
обеспечения информационной безопасности
пользователями при работе с корпоративными
информационными ресурсами
ООО «Клиника гормонального здоровья»

Хабаровск

Оглавление

Термины, сокращения и определения.....	3
1. Цель.....	4
2. Область применения.....	4
3. Общие положения.....	4
4. Автоматизированное рабочее место	4
5. Аутентификация пользователя	6
6. Электронная почта.....	7
7. Интернет и сети общего пользования	9
8. Инциденты информационной безопасности	10
9. Ответственность	11

Термины, сокращения и определения

Наименование термина	Сокращение	Определение термина / (расшифровка сокращения)
Информационные ресурсы	–	Совокупность данных и информации, представленных в различных формах и используемых для удовлетворения информационных потребностей пользователей
Положение	–	Положение об информационной безопасности ООО «Клиника гормонального здоровья»
Правила	–	Правила обеспечения информационной безопасности пользователями при работе с корпоративными информационными ресурсами ООО «Клиника гормонального здоровья»
Рабочая информация	–	Любая информация, используемая в процессе деятельности Общества
Сотрудники технической поддержки и администраторы	–	Работники Общества и третьи лица, в функции которых входят задачи по оказанию помощи пользователям в решении технических вопросов, связанных с использованием ИТ-инфраструктуры Общества, на основании созданных заявок
Устройство аутентификации	–	Техническое (аппаратное) устройство, содержащее информацию о его владельце, которая может использоваться при идентификации и аутентификации
Должностные обязанности	–	Трудовые функции, предусмотренные для работника в соответствии с трудовым договором и (или) для третьих лиц в соответствии с условиями договоров и (или) соглашений
АРМ	-	Автоматизированное рабочее место пользователя
ПДн	-	Персональные данные

1. Цель

Целью настоящего документа является определение правил обеспечения ИБ при работе пользователя в ИТ-инфраструктуре Общества.

2. Область применения

Правила распространяются на пользователей ИТ-инфраструктуры Общества.

3. Общие положения

3.1. Правила разработаны с учетом исполнения законодательных требований в сфере обеспечения ИБ, особенностей реализации применяемых технологий и способов обработки защищаемой информации в Обществе.

3.2. Пользователь обязан соблюдать настоящие требования Правил по использованию АРМ, корпоративной электронной почты и сети Интернет, обеспечению конфиденциальности аутентификационной информации, а также сообщать о подозрениях на инциденты ИБ.

3.3. Информация, обрабатываемая в ИТ-инфраструктуре Общества, считается собственностью Общества, если иное не оговорено соответствующими договорами и (или) соглашениями.

3.4. Общество оставляет за собой право протоколировать и контролировать действия пользователей при обработке информации в ИТ-инфраструктуре.

4. Автоматизированное рабочее место

4.1. Пользователю должен предоставляться АРМ с предустановленным минимально необходимым набором ПО.

4.2. Доступ к элементам ИТ-инфраструктуры Общества на АРМ осуществляется через корпоративную сеть передачи данных.

4.3. АРМ предоставляется пользователям во временное пользование и должен использоваться только для исполнения должностных обязанностей.

4.4. Доступ к ИТ-инфраструктуре предоставляется работникам Общества для выполнения должностных обязанностей или третьим лицам на основании условий договоров и (или) соглашений, заключенных между Обществом и третьими лицами.

4.5. Пользователям запрещается самостоятельно создавать, устанавливать, настраивать, отключать или удалять ПО, а также вскрывать корпус и изменять конфигурацию АРМ. Для внесения изменений в состав ПО и (или) аппаратных средств нужно обращаться к администратору.

4.6. В случаях, обусловленных производственной необходимостью, пользователю могут быть предоставлены расширенные права, позволяющие создавать, устанавливать разрешенное к использованию в Обществе ПО, настраивать, отключать или удалять ПО и (или) изменять конфигурацию АРМ.

4.7. Пользователь с расширенными правами несет ответственность за работоспособность АРМ в случае изменения настроек АРМ, установки, настройки, отключения или удаления ПО.

4.8. Пользователю запрещается самовольно устанавливать и запускать любые средства фильтрации трафика, шифрования данных, средства подбора и восстановления паролей, анализа трафика, средства сканирования сетей, средства удаленного администрирования, а также любое потенциально вредоносное ПО, если иное не предусмотрено выполнением должностных обязанностей. Запрещается устанавливать и запускать любое нелицензионное ПО. Невыполнение требований настоящего пункта Правил является основанием для лишения пользователя расширенных прав.

4.9. Вся рабочая информация должна храниться на информационных ресурсах Общества.

4.10. Пользователь обязан соблюдать установленные в Обществе правила работы с документами, порядок их учета, хранения и уничтожения.

4.11. Для обеспечения сохранности рабочей информации пользователю рекомендуется проводить резервное копирование. Разрешается выполнять копирование рабочей информации только на специально предназначенные для этого информационные ресурсы Общества или на учтенные в Обществе носители информации в соответствии с установленными в Обществе процедурами. Сохранность информации, хранимой на АРМ, не гарантируется. Ответственность за потерю информации, хранимой на АРМ, несет пользователь.

4.12. Пользователь обязан следить за чистотой и порядком организованного рабочего места.

4.13. Покидая рабочее место, пользователь обязан заблокировать доступ к работающему АРМ (Win+L).

4.14. По окончании работы документы и иные носители конфиденциальной информации ограниченного доступа (ПДн), необходимо убирать в сейф или запирающиеся шкафы.

4.15. Запрещается осуществлять копирование, в том числе методом фото- и видеосъемки, а также распространение, перепечатка (целиком или частично) или иное использование рабочих документов или экранов АРМ, с выведенной на них рабочей информацией, если иное не предусмотрено должностными обязанностями.

4.16. Пользователю запрещается:

- самостоятельно изменять режим работы, в том числе отключать, средства защиты информации;
- несанкционированно подключать к ИТ-инфраструктуре Общества любое оборудование (активное сетевое оборудование и прочее), периферийное оборудование (модемы, сканеры, принтеры, внешние запоминающие устройства, смартфоны и т. д.);

- без советующего разрешения подключаться с АРМ к внешним компьютерным сетям, в том числе, используя для этого телефоны, модемы, устройства беспроводного доступа и иное сетевое оборудование;
- умышленно использовать недокументированные свойства и ошибки в ПО или в настройках средств защиты информации. Об обнаружении такого рода ошибок и (или) эксплуатации необходимо информировать администратора сети, реализующего функции по обеспечению ИБ в Обществе, путем направления письма на адрес **admin@vesu-net.com**;
- осуществлять действия, направленные на преодоление систем информационной безопасности для получения доступа к ИТ-инфраструктуре Общества в обход установленных правил, в том числе осуществлять перехват, сокрытие, туннелирование сетевого трафика;
- оставлять мобильные устройства хранения информации (ноутбуки, планшеты, оптические диски, внешние носители информации и т. п.) без личного присмотра в местах, где существует риск несанкционированного доступа или их утраты;
- копировать и хранить информацию ограниченного доступа на носителях информации в обход установленных в Обществе правил;
- хранить документы и проекты документов в местах общего доступа;
- просматривать, хранить и обрабатывать любую информацию, не относящуюся к исполнению должностных обязанностей;
- выполнять действия для элементов ИТ-инфраструктуры Общества, под диктовку кого-либо по телефону;
- допускать к работе на АРМ лиц, не являющихся пользователями Общества и/или не имеющих прав доступа к ИТ-инфраструктуре;
- предоставлять доступ к АРМ под учетной записью пользователя только при возникновении инцидентов, для решения которых требуется привлечение администратора Общества;
- подключаться к ИТ-инфраструктуре, когда не исключена возможность нахождения вредоносного ПО на подключаемом оборудовании;
- подключаться к ИТ-инфраструктуре с личных компьютеров пользователей и третьих лиц, а также другого оборудования, когда такое подключение не согласовано в соответствии с установленными в Обществе процедурами.

5. Аутентификация пользователя

5.1. Для защиты от несанкционированного доступа к ИТ-инфраструктуре Общества пользователь должен использовать аутентификационную информацию (пароли, СМС-коды, QR-коды и т. д.) и (или) устройства аутентификации (токены, смарт-карты и т. д.), в том числе с использованием личным мобильных устройств.

5.2. В целях обеспечения двухфакторной аутентификации пользователь предоставляет номер своего мобильного телефона для получения необходимой аутентификационной информации.

5.3. С целью соблюдения принципа персональной ответственности за свои действия каждому пользователю, допущенному к работе в ИТ-инфраструктуре Общества, назначается индивидуальная учетная запись.

5.4. Пользователю запрещается использовать чужую учетную запись и (или) передавать кому-либо свои средства и данные аутентификации. Использование чужой учётной записи может быть расценено как незаконное проникновение в информационную систему или мошенничество.

5.5. Пользователь обязан сменить пароль при первом входе (если такая возможность обеспечена элементом ИТ-инфраструктуры), а также использовать в дальнейшем пароли, руководствуясь требованиями политики управления аутентификацией Общества с учетом законодательных требований в сфере обеспечения ИБ, применяемых технологий и способов обработки защищаемой информации.

5.6. Пользователи обязаны обеспечить безопасное хранение и использование аутентификационной информации и устройств аутентификации, исключая их утерю или разглашение.

5.7. Устройства аутентификации должны храниться в месте, недоступном для посторонних лиц. Для этого можно использовать сейф, специальный контейнер или другое надёжное хранилище.

5.8. Пользователю запрещается сообщать и (или) передавать кому-либо, свою аутентификационную информацию и устройства аутентификации, предназначенные для доступа к ИТ-инфраструктуре Общества.

5.9. В случае подозрения на компрометацию и (или) утраты аутентификационной информации (учетные данные) или устройства аутентификации необходимо:

- сменить аутентификационную информацию (если это возможно) и (или) применить меры по поиску и блокировке аутентификационной информации (учетные данные, сертификат) на устройствах аутентификации;
- проинформировать об инциденте непосредственного руководителя и администратора Общества, путем направления письма на адрес **admin@vesu-net.com**.

6. Электронная почта

6.1. При использовании электронной почты пользователю запрещается:

- указывать персональный корпоративный адрес электронной почты на общедоступных сайтах и использовать адрес корпоративной электронной почты для регистрации и (или) получения услуг в сети Интернет, не связанных с выполнением должностных обязанностей;

- пересылать письма корпоративной электронной почты на внешние адреса электронной почты, за исключением случаев, когда это требуется для выполнения служебных обязанностей;
- использовать для корпоративной переписки личные почтовые ящики, зарегистрированные в публичных системах электронной почты (например, Yahoo, Mail.ru, Gmail и др.);
- осуществлять массовую рассылку сообщений по электронной почте в сети Интернет;
- отправлять сообщения противозаконного, враждебного или неэтичного содержания;
- самовольно менять настройки клиента электронной почты, за исключением действий, предусмотренных корпоративными инструкциями по эксплуатации данного ПО;
- использовать электронную почту для пересылки информации ограниченного доступа.

6.2. При использовании электронной почты пользователь обязан:

- использовать корпоративную электронную почту только для выполнения своих должностных обязанностей;
- при получении писем, вызывающих подозрение (не открывая их), информировать непосредственного руководителя и администратора Общества, путем направления письма на адрес **admin@vesu-net.com**.
- отвечать и предпринимать действия, указанные в письме, необходимо только убедившись в подлинности и корректности полученного письма и его отправителя;
- проверять подлинность и корректность полученных писем перед тем, как на них отвечать или предпринимать действия;
- в случае необходимости настройки клиента электронной почты обращаться к администратору Общества.

6.3. Владелец рабочей информации самостоятельно оценивает ее конфиденциальность и принимает решение о возможности передачи по электронной почте или другими каналами передачи данных.

6.4. К признакам подозрительного письма относятся (в том числе, но не ограничиваясь):

- наличие в письме исполняемых файлов или файлов, поддерживающих выполнение произвольного кода (макроса), картинок, не относящихся к теме и содержанию письма, а также иных файлов, вызывающих подозрение;
- сомнительное содержание письма (экстремистская информация, призывы к действиям, не относящимся к исполнению должностных обязанностей);
- наличие в теле письма ссылок и гиперссылок, ведущих на неизвестные, запрещенные или сомнительного содержания сайты, путей к папкам и файлам и прочее;

– письмо получено от неизвестного отправителя, который просит выполнить действия в ИТ-инфраструктуре Общества.

7. Интернет и сети общего пользования

7.1. При использовании ресурсов сети Интернет пользователям запрещается:

- использовать ресурсы Интернет в личных целях;
- посещать ресурсы Интернет, содержащие материалы противозаконного, экстремистского или неэтического характера, использовать доступ в Интернет в развлекательных целях;
- раскрывать конфиденциальную информацию Общества, путем размещения ее на общедоступных ресурсах Интернет;
- использовать Интернет для несанкционированной передачи или получения информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;
- предпринимать действия, направленные на получение несанкционированного доступа к защищенным ресурсам Интернет;
- использовать системы мгновенного обмена сообщениями, системы передачи голоса по IP-протоколу, системы видеосвязи по IP-протоколу и системы для удаленного доступа, за исключением корпоративных систем, разрешенных для использования в Обществе;
- использовать сервисы мгновенного обмена сообщениями, электронной почты, передачи голоса и видеосвязи, удаленного доступа в целях передачи через сеть Интернет информации, доступ к которой ограничен федеральными законами, внутренними ЛНА, а также иными соглашениями (договорами);
- использовать для хранения рабочей информации публичные сервисы хранения данных.

7.2. Все полученные через сеть Интернет файлы необходимо проверять средствами антивирусной защиты.

7.3. Техническое обслуживание производится в целях устранения неполадок, установки и настройки ПО и оборудования и выполняется по заявке пользователя администратору.

7.4. Локальное техническое обслуживание проводится на АРМ пользователя в его присутствии.

7.5. Дистанционное техническое обслуживание используется для ускорения обработки заявок и осуществляется с рабочего места специалиста, уполномоченного на выполнение соответствующего вида работ.

7.6. Перед разрешением удаленного подключения пользователь должен закрыть все свои рабочие файлы, а также окна используемых приложений, за исключением приложения, по которому проводится техническое обслуживание.

7.7. Пользователь должен видеть все действия, осуществляемые при дистанционном техническом обслуживании (перемещения мыши, копирование файлов, открытие окон и т. д.).

7.8. Пользователь должен прервать сеанс дистанционного технического обслуживания в случаях:

- выполнение сотрудником технической поддержки подозрительных действий, не связанных с решением проблемы;
- необходимости покинуть рабочее место;

8. Инциденты информационной безопасности

8.1. Пользователь может являться участником процесса решения инцидентов ИБ.

8.2. Пользователь обязан немедленно сообщить об инциденте ИБ путем направления сообщения по адресу администратора Общества **admin@vesu-net.com**, в случае:

- оказания внешнего воздействия на пользователя (в том числе угроз) со стороны коллег или лиц, представляющих таковыми, при попытках получить доступ к АРМ, ИТ-инфраструктуре Общества или конфиденциальной информации;

- выявления инцидентов ИБ, подозрения на них или выявления несанкционированного сбора информации.

8.3. К инцидентам ИБ относятся (в том числе, но не ограничиваясь):

- несанкционированный доступ посторонних лиц к техническим средствам и прочим защищаемым местам;

- утрата или хищение носителей конфиденциальной информации;

- получение доступа к информации, которая, по мнению работника, не должна быть ему доступной;

- заражение компьютера вирусами или появление признаков заражения;

- сбой технических средств, повлекшие за собой выход из строя накопителей, содержащих конфиденциальную информацию;

- попытки получения посторонними лицами, в том числе представляющимися работниками Общества, конфиденциальной информации;

- разглашение учетных данных, потеря, кража устройств аутентификации;

- несанкционированное изменение настроек программных и (или) аппаратных средств АРМ и ИТ-инфраструктуры;

- подозрительная активность на АРМ:

- самопроизвольное изменение места положения курсора;

- неожиданная смена картинки экрана;

- значительное увеличение времени отклика компьютера;

- необъяснимая потеря файлов;

- изменение дат изменения файлов;
- нетипичное изменение атрибутов или размера файлов.
- обнаружение защищаемой информации у лиц, не имеющих доступа к ней, а также в открытом доступе, в том числе в социальных сетях и электронных средствах массовой информации.

9. Ответственность

9.1. Ответственность за исполнение требований Правил возлагается на всех работников Общества.

9.2. В соглашения с третьими лицами, в рамках которых осуществляется предоставление доступа третьим лицам к ИТ-инфраструктуре Общества, должны включаться требования о необходимости соблюдения третьими лицами положений Правил.

9.3. Лица, нарушившие требования Политики, несут ответственность в соответствии с действующим законодательством Российской Федерации, внутренними документами Общества и условиями договора, заключенного между Обществом и работником или третьими лицами.