

Правила информационной безопасности

1. Соблюдение требований при работе на автоматизированном рабочем месте

1.1. Сотрудники обязаны

- при отсутствии визуального контроля блокировать доступ к АРМ (одновременное нажатие комбинации клавиш «Win + L», «Ctrl + Alt + Del» и выбор опции <Блокировка> либо блокировка доступа иным способом, предусмотренным в операционной системе);
- по окончании рабочего дня выключать АРМ, кроме случаев, необходимых для выполнения своих должностных обязанностей и резервного копирования АРМ;
- располагать экран монитора во время работы на АРМ в помещении так, чтобы исключалась возможность ознакомления посторонних лиц с визуальной отображаемой информацией на экране монитора;
- по окончании печати забирать распечатанные документы с сетевых печатающих устройств;
- пользоваться только зарегистрированными (учтенными) съемными машинными носителями информации;
- обеспечивать безопасное хранение материальных носителей информации, исключающее несанкционированный доступ к ним;
- незамедлительно сообщать руководителю о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) информации;
- соблюдать установленный режим разграничения доступа к информационным ресурсам;
- в случае увольнения сдавать съемными машинными носители информации.

1.2. Сотрудникам запрещается

- разглашать любым способом третьим лицам идентификационные и аутентификационные данные (логины, пароли, секретные ключи) и атрибуты доступа к информационным и техническим ресурсам;
- использовать ставшие известными учетные записи других сотрудников;
- использовать предоставленные технические средства и ресурсы в целях, не связанных с исполнением работником своих должностных обязанностей;
- подключать к корпоративной сети АСР и АРМ, посторонние технические средства, в том числе мобильные устройства (планшеты, смартфоны

и т.п.), иные не зарегистрированные съемные машинные носители информации, а также личное оборудование (ноутбуки, компьютеры);

- копировать информацию, ставшую им известной в ходе выполнения должностных обязанностей на личные носители информации без служебной необходимости.

- оставлять во время работы материальные носители информации без присмотра, не санкционированно передавать их посторонним лицам и выносить без регистрации перемещения за пределы помещений, в котором производится обработка защищаемой информации;

- использовать внутри периметра корпоративной сети АСР сторонние (в том числе публичные) каналы доступа в Интернет на служебных АРМ, в т. ч. подключаться к мобильным и сторонним беспроводным сетям передачи данных;

- создавать с использованием программных или аппаратных средств дополнительные каналы обмена информацией с внутренними или внешними абонентами, в том числе с использованием некорпоративных внешних ресурсов;

- самовольно организовывать беспроводные точки доступа внутри периметра корпоративной сети АСР;

- самовольно вносить изменения в настройки операционных систем, конфигурацию программно-аппаратных средств АРМ, в том числе устанавливать ПО и обновления;

- использовать штатные средства операционных систем, а также любое другое программное обеспечение для проведения сканирования сети, несанкционированного доступа и выполнения других подобных действий;

- самовольно создавать общие ресурсы на АРМ;

- использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации, компьютерным инцидентам или сбоям в работе корпоративной сети АСР;

- предоставлять третьим лицам несанкционированный доступ к АРМ и ресурсам организации, регистрационным данным, секретным кодам и сведениям, раскрывающим структурные элементы организации инженерной инфраструктуры АСР;

- использовать любое нелицензионное и не разрешенное к применению УИТиЦР программное обеспечение;

- самовольно создавать виртуальные машины, несколько загрузочных копий операционных систем, производить загрузку рабочей станции с внешних носителей информации;

- отключать (блокировать, удалять) корпоративные средства администрирования и средства защиты, установленные на АРМ;

- запускать исполняемые файлы, полученные не из достоверных источников, без согласования с УИТиЦР и проверки средствами антивирусной защиты;
- регистрироваться и работать в корпоративной сети АСР под чужим логином и паролем или чужим идентификатором доступа;
- обрабатывать информацию с использованием зарубежных сервисов (Google, Yahoo и т.п.);
- разрабатывать (создавать) служебные документы (официальные письма, служебные записки и другие документы) с использованием чат-ботов с искусственным интеллектом (например, ChatGPT и его аналогов).
- самостоятельно устанавливать, тиражировать, или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- открывать файлы, поступившие из неизвестных внешних источников, в том числе вложенные файлы входящих сообщений электронной почты, файлы, размещенные на съемных носителях информации, файлы, загруженные из информационно-телекоммуникационной сети «Интернет», без предварительной проверки антивирусными средствами;
- отправлять по открытым каналам связи защищаемую информацию, если информация не зашифрована сертифицированными средствами криптографической защиты информации;
- привлекать лиц, не являющихся сотрудниками, для установки программного обеспечения, ремонта или настройки технических средств, за исключением случаев, когда данные услуги оказываются на договорной.
- осуществлять фото- и видео съемку рабочих документов, а также публикацию таких документов в социальных сетях и других открытых ресурсах (за исключением случаев, когда это необходимо для выполнения должностных обязанностей).

2. Соблюдение требований парольной защиты

2.1. При формировании пароля необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее 8-и буквенно-цифровых символов;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, общепринятые сокращения) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о Сотруднике;

- в числе символов пароля, обязательно должны присутствовать цифры и буквы в верхнем и нижнем регистрах;
- запрещается использовать в качестве пароля
 - ✓ один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например «123123», «111»);
 - ✓ комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, qwerty», 1234567 и т.п.);
 - ✓ ранее использованные пароли.

2.2. Для организации парольной защиты Сотруднику запрещается:

- хранить пароли в записанном виде на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- сообщать свои идентификационные данные и пароли другим сотрудникам и посторонним лицам, а также разглашать сведения о применяемых способах и методах защиты информации, а также средствах защиты информации
- использовать пароль доступа к корпоративной вычислительной сети в других программах и на сайтах, требующих регистрации.

2.3. При утрате, компрометации ключевой, парольной и аутентифицирующей информации незамедлительно произвести их смену.

2.4. Внеплановая смена личного пароля производится в обязательном порядке в следующих случаях:

- компрометации (подозрении на компрометацию) пароля;
- прекращения полномочий (увольнение, переход на другую работу внутри организации) Сотрудника (в течение 24 часов после окончания последнего сеанса работы);

3. Соблюдение требований антивирусной защиты информации

3.1. Сотрудник обязан:

3.1.1. В случае появления подозрений на наличие вредоносного программного обеспечения (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) или выявления фактов, связанных со сбоями в работе средств защиты информации, незамедлительно провести внеочередной антивирусный контроль АРМ.

3.1.2. Проводить антивирусную проверку машинных носителей (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

3.1.3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов:

- приостановить работу с АРМ;
- выключить АРМ;

- сообщить руководителю, для дальнейшего устранения заражения.

3.2. Сотруднику запрещается:

3.2.1. Удалять или отключать средства антивирусной защиты, установленные на АРМ;

3.2.2. Вносить изменения в настройки средства антивирусной защиты, установленного на АРМ.

4. Соблюдение требований при использовании электронной почты

4.1. Сотруднику запрещается:

4.1.1. Использовать электронную почту для отправки конфиденциальной информации, информации ограниченного доступа и информации, содержащей персональные данные.

4.1.2. Использовать некорпоративную электронную почту для ведения служебной переписки.

4.1.3. Передавать учетные данные (логин, пароль) электронной почты другим Сотрудникам и третьим лицам;

4.1.4. Использовать адрес корпоративной почты для оформления подписок на сайтах, тематика которых не относится к выполнению служебных обязанностей пользователя.

4.2. Сотрудник обязан:

4.2.1. Воздерживаться от переписки с абонентами адреса которых находятся в интернет-доменах стран не дружественных Российской Федерации.

4.2.2. Осуществлять массовую рассылку адресатам корпоративной сети АСР и за ее пределы электронных сообщений, содержащих сведения, не относящиеся к выполнению функциональных обязанностей;

5. Соблюдение требований при работе в сети Интернет

5.1. При работе в сети Интернет Сотрудник обязан:

5.1.1. Производить работу исключительно в целях исполнения своих должностных обязанностей.

5.1.2. Противодействовать методам социальной инженерии: не открывать вложения в письмах от неизвестных источников, не переходить по подозрительным баннерам и ссылкам на веб-сайтах, проверять вводимый адрес веб-сайтов на предмет опечаток.

5.1.3. Обращаться к специалисту отдела информационной безопасности и системного администрирования УИТиЦР в случае выявления фактов нарушения информационной безопасности.

5.2. При работе в сети Интернет Сотруднику запрещается:

5.2.1. Посещать сайты сомнительной репутации (сайты, содержащие

нелегально распространяемое программное обеспечение, торрент-сайты, и т.д.) и скачивать с таких сайтов какие-либо файлы и программное обеспечение.

5.2.2. Загружать с сайтов сети Интернет файлы, не относящихся к служебной деятельности, в том числе аудио- и видеофайлы, а также воспроизводить аудио- и видеопотоки (сервисы онлайн-аудио, радио, онлайн-видео, телевидение).

5.2.3. Использовать несанкционированные средства обмена мгновенными сообщениями (Mail.ru-агент, IRC, ICQ, Yahoo messenger, AOL Instant Messenger и т.п.), самовольно использовать социальные сети и форумы для ведения служебной переписки.

5.2.4. Использовать программные и аппаратные средства (в т. ч. анонимные прокси-серверы и т.п.), позволяющие получить доступ к ресурсу, запрещенному к использованию политикой информационной безопасности АСР, а также для обхода ограничений по использованию ресурсов.

5.2.5. Без необходимости публиковать свой адрес электронной почты, либо адреса других сотрудников компании на общедоступных интернет-ресурсах (форумы, конференции и т.п.), информация на которых не является необходимой.

5.2.6. Утвердительно отвечать на всплывающие баннеры и предложения веб-браузера о проверке (обнаружении) компьютера на наличие вирусов, уязвимостей, установки программного обеспечения и т.п.

5.3. В случае, если должностными обязанностями Сотрудника предусмотрено использование социальных сетей и мессенджеров:

5.3.1. Использовать в социальных сетях и мессенджерах двухфакторную аутентификацию (в случае наличия технической возможности)

5.3.2. Исключить использование десктопных (компьютерных) клиентов мессенджеров и социальных сетей.

5.3.3. Не загружать конфиденциальную информацию в социальные сети и мессенджеры (в т.ч. персональные данные);

6. Соблюдение требований при работе с электронной подписью

6.1. Носители ключевой информации должны использоваться только их владельцем.

6.2. Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной ЭП операций формирования и проверки квалифицированной ЭП, шифрования и дешифрования.

Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

6.3. Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами

квалифицированной ЭП, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками

6.4. Сотрудники, эксплуатирующие электронную подпись (далее – ЭП) обязаны:

6.4.1. Обеспечить надёжное хранение носителей ключевой информации, исключающее доступ к ним посторонних лиц/

6.4.2. Для исключения несанкционированного доступа защищать ключи квалифицированной ЭП на ключевом носителе паролем (ПИН-кодом).

6.4.3. Записывать ключи квалифицированной ЭП при их создании на предварительно проинициализированные (отформатированные) ключевые носители.

6.4.4. В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной ЭП, удалять всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред организации, владельцу ЭП.

6.5. Для обеспечения безопасности ЭП Сотруднику запрещается:

6.5.1. Осуществлять несанкционированное копирование ключевых носителей.

6.5.2. Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным.

6.5.3. Выводить ключевую информацию на дисплей и принтер и иные средства отображения информации.

6.5.4. Использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя.

6.5.5. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путём переформатирования.

6.5.6. Вносить какие-либо изменения в программное обеспечение средств криптографической защиты информации и квалифицированной электронной подписи.

6.5.7. Записывать и хранить на ключевых носителях иную информацию (в том числе рабочие или личные файлы).

6.5.8. Оставлять АРМ с установленными средствами квалифицированной электронной подписи без контроля после ввода ключевой информации.

6.5.9. Удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

6.5.10. Пересылать файлы с ключевой информацией по электронной почте, сети Интернет или по внутренней электронной почте (кроме открытых ключей)

6.6. Плановая смена ключей и сертификатов открытых ключей осуществляется пользователем самостоятельно.

6.7. Внеплановая замена ключей и сертификатов закрытых ключей проводится в случае:

- компрометации ключей (утрата ключевых носителей ключа; утрата носителей ключа с последующим обнаружением; увольнение сотрудников, имевших доступ к ключевой информации);
- изменения идентификационных данных и/или областей использования ключа, указанных в заявлении на изготовление ключей;
- выхода из строя ключевого носителя.

7. Соблюдение требований при удаленном доступе к ресурсам корпоративной сети или удаленной (дистанционной) работе

7.1. При использовании удаленного доступа Сотрудник обязан:

7.1.1. Выбирать места удаленной работы с учетом обеспечения защиты АРМ.

7.1.2. Завершать сеансы удаленной работы после окончания их использования.

7.1.3. Регулярно, не реже одного раза в день, на используемых для удаленного доступа АРМ, обновлять антивирусные базы.

7.2. При использовании удаленного доступа Сотруднику запрещается:

7.2.1. Предоставлять неавторизованный доступ к информации или ресурсам корпоративной сети АСР третьим лицам, в том числе близким пользователю людям (членам семьи, друзьям).

7.2.2. Оставлять без присмотра в незащищенном месте АРМ, используемый для удаленного доступа.

7.2.3. Использовать средства удалённого доступа к ресурсам и сервисам корпоративной сети АСР, не согласованные УИТиЦР.

7.3. При установлении удаленного (дистанционного) режима работы настоящие правила соблюдаются Сотрудниками в полном объеме.

8. Соблюдение требований при проведении совещаний в формате Видеоконференции

8.1. Исключить использование Сотрудниками в служебных целях иностранных сервисов для проведения видеоконференций (Zoom, Skype, и др.) в ходе исполнения должностных обязанностей.

9. Ответственность за нарушение правил информационной безопасности

9.1. Каждый Сотрудник несет ответственность за нарушение правил

информационной безопасности в пределах своих служебных обязанностей и полномочий.

9.2. Сотрудник несет персональную ответственность за:

- соблюдение требований настоящих правил;
- свои действия и бездействие при выполнении своих должностных и функциональных обязанностей и информационном взаимодействии с третьими лицами;
- достоверность и полноту информации, которая обрабатывается пользователем с использованием АРМ;

9.3. Нарушение настоящих Правил может повлечь за собой ограничение доступа к защищаемой информации и прекращение обработки информации на АРМ.

9.4. Нарушение данных Правил, повлекшее неправомерное уничтожение, блокирование, модификацию либо копирование охраняемой законом информации, нарушение работы информационных систем и ресурсов, может повлечь дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

9.5. На основании ст. 192 Трудового кодекса Российской Федерации Сотрудники, нарушающие правила настоящего документа, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

9.6. На основании ст. 238 Трудового кодекса РФ все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный ОМС СР в результате нарушения ими правил настоящего документа.

9.7. На основании ст. 81 Трудового кодекса Российской Федерации с Сотрудником может быть расторгнут трудовой договор, в случае разглашения сотрудником охраняемой законом тайны (коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого сотрудника.

9.8. Взаимодействие между Сотрудниками и иными лицами по вопросам информационного взаимодействия, исполнения требований по обеспечению информационной безопасности в соответствии со служебными отношениями, регламентируются локальными организационно-распорядительными документами, положениями о структурных подразделениях, должностными инструкциями и иными документами, в том числе по вопросам защиты информации.