Приложение
к служебному письму

[redacted] № [redacted]

Инструкция по кибергигиене на автоматизированном рабочем месте

1. Учётные записи и пароли сотрудника

Для каждого сотрудника создаётся персональная учётная запись, в которую входит логин и пароль. Персональная учётная запись необходима для авторизации сотрудника в информационных системах и подтверждения действий, совершённых авторизованным пользователем.

Сотрудник несёт персональную ответственность за действия, совершённые под его персональной учётной записью.

Чтобы защитить себя, своё рабочее место и свою персональную учётную запись, есть ряд правил, которые должны соблюдаться всеми сотрудниками, использующими для выполнения должностных обязанностей средства вычислительной техники – автоматизированные рабочие места (далее – АРМ):

– знать требования руководящих документов по защите информации и настоящей Инструкции;

– никому не передавать и не сообщать свои персональные логин и пароль, электронные идентификаторы, Pin-коды и т. д.;

– не пользоваться чужими учётными записями и паролями;

– использовать сложные пароли и производить их замену каждые три месяца;

– не хранить пароли в доступных местах (блокнот, монитор, коврик для мыши, клавиатура);

– АРМ, на котором работает сотрудник не должно оставаться без присмотра, так как за сохранность отвечает сам сотрудник;

– при потере пароля и электронного идентификатора или невозможности войти в учётную запись под своим паролем, необходимо немедленно сообщить об этом сотруднику или руководителю, ответственному за защиту информации;

– не использовать пароль от корпоративной персональной учётной записи в других местах, где требуется регистрация;

– личный пароль разрешается хранить в опечатанном конверте (тубусе) в сейфе у начальника подразделения или его заместителя;

– разрешается хранить пароль на специальном защитном устройстве (например, Rutoken, E-token, Esmart USB, JaCarta LT, JaCarta-2 SE и т. д.);

– устройства Rutoken, E-token, Esmart USB, JaCarta LT, JaCarta-2 SE необходимо хранить в индивидуальном запираемом и опечатываемом сейфе, в случае отсутствия сейфа разрешается хранить в опечатанном конверте (тубусе) в сейфе у начальника подразделения или его заместителя, сделав соответствующую запись в журнале учёта выдачи ключевых носителей.

1.1. Установлены следующие требования в отношении паролей:

Личные пароли должны выбираться пользователями АРМ самостоятельно с учётом следующих требований:

1. Длина пароля должна быть не менее 8 символов.

2. В числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, %, иные).

3. Символы паролей должны вводиться в режиме латинской раскладки клавиатуры.

4. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ, иное), а также общепринятые сокращения (ЭВМ, ЛВС, USER, иное).

5. Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также свои имя и дату рождения, имя и дату рождения своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о сотруднике.

6. Запрещается использовать в качестве пароля один и тот же повторяющийся символ, либо повторяющуюся комбинацию из нескольких символов.

7. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т. п.).

8. Запрещается выбирать пароли, которые уже использовались ранее.

9. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях.

10. Личный пароль сотрудник не имеет права (и не должен) сообщать никому.

11. Смена паролей сотрудников должна проводиться регулярно, не реже одного раза в 30 дней во всех информационных системах, к которым сотрудник имеет доступ.

12. Контроль за действиями сотрудников при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на сотрудника и руководителя, ответственного за защиту информации.

13. Внеплановая смена личного пароля или удаление учётной записи сотрудника производится владельцем системы после его уведомления руководителем структурного подразделения увольняемого сотрудника или лицом, ответственным за защиту информации.

2. Правила пользования сетью Интернет

Сотрудник должен использовать сеть Интернет только:

– в рамках исполнения своих должностных обязанностей исключительно с включёнными средствами защиты информации (антивирус Dr. Web);

– для повышения профессиональной квалификации;

– для осуществления обмена сообщениями и документами с сотрудниками с использованием корпоративной электронной почты.

Что запрещено сотруднику делать в сети Интернет:

– работать при выключенных средствах защиты;

– скачивать из сети Интернет программное обеспечение и другие файлы, которые могут нанести вред вашему оборудованию (торренты, файлы с расширением «.exe, .rar, .zip, .js, .scr» и т. п.);

– посещать сайты, не связанные с выполнение должностных обязанностей (социальные сети, интернет-магазины, сервисы потокового видео, сервисы бесплатной электронной почты и т. д.);

– пользоваться личной электронной почтой, личным аккаунтом в социальных сетях и мессенджерах для пересылки служебных сообщений;

– использовать игровые сервисы и приложения, torrent-клиенты, майнинг, утилиты удалённого администрирования.

3. Правила использования электронной почты

Электронная почта предоставляется работникам только для исполнения своих служебных обязанностей.

Использование ее в личных целях запрещено!

При использовании корпоративной электронной почты запрещается пересылать информацию ограниченного доступа (персональные данные, информацию для служебного пользования), а также пересылать нелегально распространяемые материалы (аудио- и видеоданные, программное обеспечение, письма с сомнительными вложениями, такими как поздравительные открытки, подарочные карты, сертификаты на приобретение товаров и т. п.).

Нельзя указывать служебные электронные адреса в общедоступных ресурсах сети Интернет (блоги, форумы и т. п.), если это не связано со служебной необходимостью.

Необходимо использовать корпоративную электронную почту **ТОЛЬКО** в рабочих целях, для обмена служебными сообщениями и документами.

СТРОГО ЗАПРЕЩЕНО:

– производить рассылку материалов рекламного (непрофильного) и развлекательного характера;

– производить массовую рассылку писем непроизводственного характера;

– пересылать исполняемые файлы (с расширениями .exe, .dll, .pif и т. п.);

– пересылать мультимедийные файлы (аудио и видео);

– производить рассылку вредоносных программ или файлов, заражённых вирусами;

– переходить по ссылкам, которые содержаться в электронных письмах, особенно если они длинные, или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т. д.);

– нажимать на ссылки из писем, если они заменены на слова;

– нажимать на ссылки из писем и просматривать полный адрес сайта;

– открывать вложения, особенно если в них содержатся документы с макросами, архивы с паролями, файлы с расширениями RTF, LNK, CHM, VHD;

– открывать письма от неизвестных адресатов;

– осуществлять деятельность, нарушающую законы и нормативные правовые акты Российской Федерации;

– предоставлять кому-либо логин и пароль для доступа к своей корпоративной электронной почте.

4. Установка программного обеспечения на АРМ

В технических средствах АРМ необходимо использовать только лицензионное программное обеспечение фирм-изготовителей, полученное из доверенных источников.

При необходимости установки дополнительного программного обеспечения необходимо согласовать с руководителем структурного подразделения и ответственным за защиту информации возможность его использования, после чего направить соответствующую заявку в службу поддержки пользователей «Service Desk», адрес ресурса: **https://help.belregion.ru**

Сотрудник в части касающейся обязан знать порядок эксплуатации программного обеспечения и уметь правильно его применять в ходе исполнения должностных обязанностей.

Ознакомление и обучение сотрудников работе с программным обеспечением в пределах выполняемых функций проводит руководитель подразделения или сотрудник владельца информационной системы.

Необходимо исключить попадание в операционную систему средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также программ, позволяющих получать привилегии администратора.

В случае обнаружения программного обеспечения, не входящего в список доверенных программ и не предназначенного для выполнения служебных обязанностей, сотрудник обязан немедленно прекратить работу и проинформировать руководителя или ответственного за защиту информации и направить заявку в службу поддержи на удаление вышеуказанного программного обеспечения.

Пользователям, не являющимся сотрудниками ИТ-подразделений, назначаются минимально необходимые права и привилегии, нужные для выполнения должностных обязанностей.

5. Правила пользования антивирусной защитой

В целях защиты информации от вредоносных программ на автоматизированном рабочем месте устанавливается антивирусное программное обеспечение Dr.Web, которое настроено администратором для осуществления эффективной антивирусной защиты (обновление антивирусных баз и сканирование операционной системы происходит в автоматическом режиме по заранее запланированному графику, настройки политики безопасности также находятся под управлением администратора, ***не пытайтесь настроить антивирус Dr.Web самостоятельно!***).

Для проверки файла или папки с файлами нужно выполнить ряд действий:

1. Зайти в папку, где расположен файл или папки с файлами (рис. 1) или же открыть интерфейс антивируса Dr.Web, в появившемся окне слева будет текст «Перетащите сюда файлы или нажмите для выбора» (рис. 2), перетащите файл для проверки, после чего начнется проверка.

2. Также можно нажать правой кнопкой мыши по названию проверяемого файла или папки с файлами. После этого появится меню, где необходимо выбирать пункт «Проверить Dr.Web» (рис. 1).

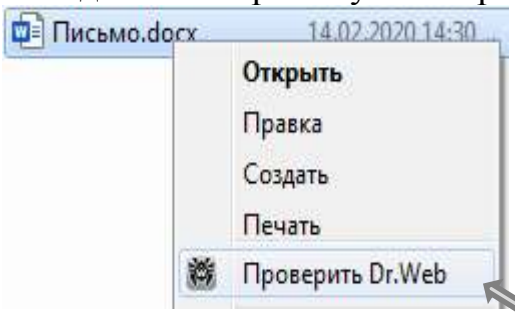

Рис. 1. Проверка файла через Dr.Web.

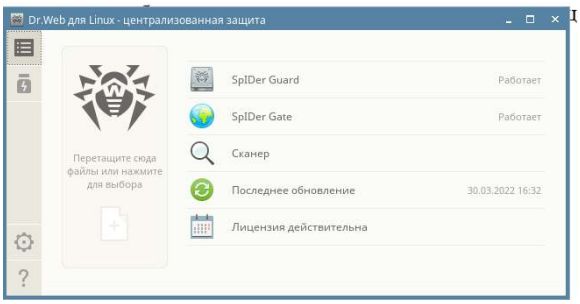

Рис. 2. Проверка файла через Dr.Web.

3. В открывшемся окне будет видно, как антивирус проверяет файл или папку с файлами на наличие угроз.

4. По окончании сканирования в окне отображается результат проверки с указанием обнаруженных объектов и угроз.

5. В случае обнаружения сканером угроз он предложит их обезвредить, для этого необходимо нажать кнопку «Обезвредить».

6. В случае обнаружения вредоносного программного обеспечения на АРМ, не поддающегося лечению антивирусной программой, сотрудник обязан немедленно поставить в известность руководителя или ответственного за защиту информации, прекратить обработку информации на АРМ и направить в обязательном порядке соответствующую заявку в службу поддержки. В свою очередь, ответственный за защиту информации должен убедиться в актуальности используемых антивирусных баз и уведомить отдел информационной безопасности департамента инфраструктурных решений министерства цифрового развития Белгородской области о выявленных фактах. Работа на АРМ запрещается до решения вопроса о возможности дальнейшей его эксплуатации.

В процессе своей работы Dr.Web автоматически проверяет все сообщения электронной почты, проходящие через сервер. При этом проверяются файлы вложений, а также все объекты OLE, встроенные в документы. При обнаружении вирусов в почтовом сообщении тело вируса изымается и перемещается в зону карантина, после чего администратору сервера приходит извещение (рис. 3).

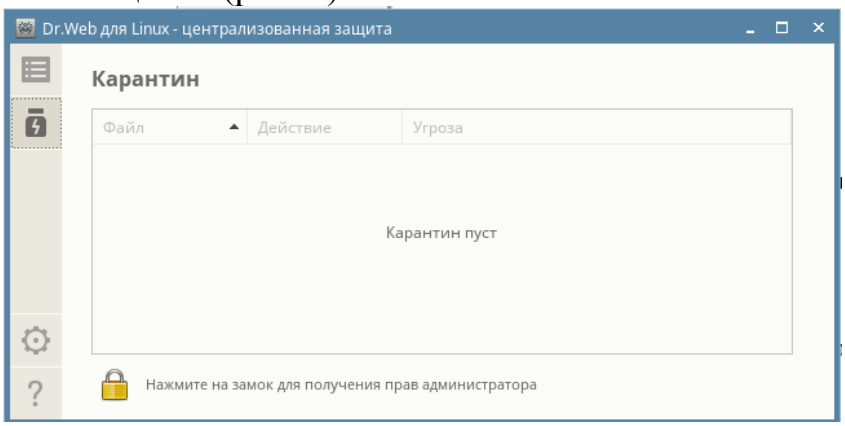

Рис. 3 Интерфейс антивирусного программного обеспечения Dr.Web.

Сотрудник может обратиться в службу поддержки для проверки и оценки файла на предмет угроз безопасности информации либо перенаправить сообщение на электронный почтовый ящик (avz@belregion.ru), где будет проведена проверка сообщения на предмет наличия известных угроз информационной безопасности.

6. Обращение с ключевой информацией (электронной подписью)

Необходимо:

– хранить в тайне закрытый ключ электронной подписи (далее – ЭП);

– немедленно приостанавливать действия сертификата ключа проверки ЭП при наличии оснований полагать, что тайна закрытого ключа ЭП нарушена (произошла компрометация ключа);

– обновлять сертификат ключа проверки ЭП в соответствии с регламентом удостоверяющего центра, выдавшего сертификат;

– хранить электронную подпись только на специальных ключевых носителях, таких как Rutoken, E-token, Esmart USB, JaCarta LT,JaCarta-2 SE.

Ключевой носитель должен быть зарегистрирован в журнале учёта ключевых носителей и храниться в опечатанном служебном сейфе, а при отсутствии условий для хранения у сотрудника ключевой носитель должен храниться в сейфе руководителя также в опечатанном виде.

Ключевой носитель подключается к АРМ только для проведения процедуры подписания документов электронной подписью. Остальное время ключевой носитель должен находиться в сейфе.

В случае утери ключевого носителя (контейнера) необходимо уведомить руководителя или ответственного за защиту информации и принять меры по отзыву сертификата ЭП. Отозвать сертификат можно посредством перехода на портал заявителя удостоверяющего центра Федерального казначейства (fzs.roskazna.ru) (рис. 4) и оформления заявки на прекращение действия сертификата.

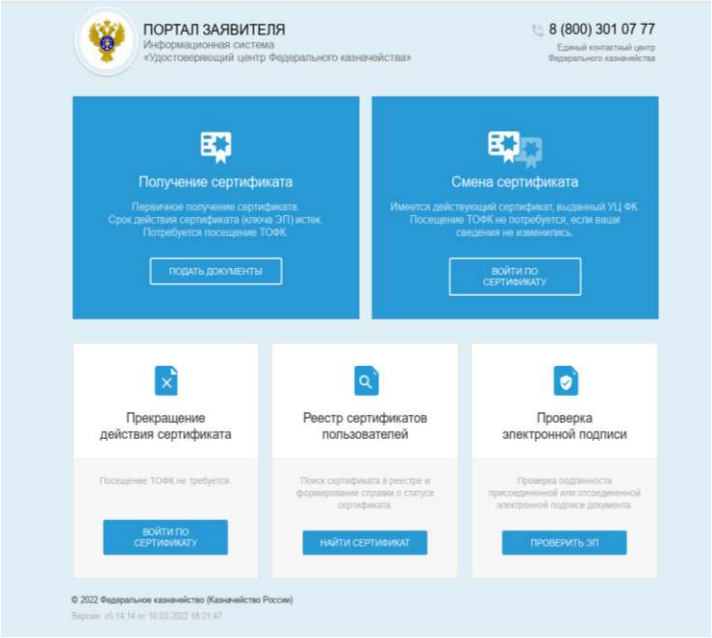

Рис. 4 Портал заявителя Удостоверяющего центра Федерального казначейства.

При необходимости на портале заявителя в установленном порядке сотрудник может подать заявку для получения нового сертификата ключа ЭП.

Сформированный ключ ЭП подлежит обязательному учёту в журнале учёта средств криптографической защиты. Журнал хранится у руководителя или сотрудника, ответственного за защиту информации.

7. Социальная инженерия, фишинг

Киберпреступники все чаще используют методы социальной инженерии для проникновения в инфраструктуру бюджетных организаций и органов власти. Человеческий фактор по-прежнему остаётся слабым звеном в любой системе защиты, поэтому сотруднику необходимо знать основы информационной безопасности.

Убеждайтесь в подлинности личности человека, звонящего Вам по телефону или контактирующего с Вами иным способом, а также в правомочности его запросов. Не предоставляйте никакой информации при первом контакте, а лично инициируйте повторный контакт.

Сохраняйте бдительность. Всегда проверяйте уровень конфиденциальности информации перед её передачей контактирующему с Вами лицу и наличие у него права на доступ к ней. Если есть сомнения, свяжитесь с техподдержкой или представителем организации, только по официально представленным данным.

Ознакомьтесь с практиками социальной инженерии и не поддавайтесь им. При получении писем по электронной почте необходимо:

1. Проверить адрес отправителя.

Сверяйте домены всех отправителей подозрительных электронных писем с доменом, указанным на официальном сайте магазина, государственного учреждения или иной организации, которые ведут с вами общение. Мошенники обычно отправляют письма с общедоступных почтовых доменов (та часть в электронном адресе, которая пишется после символа «@») – mail.ru, yandex.ru и т. п. – или используют домены, похожие на официальные доменные имена компаний, чтобы ввести получателя письма в заблуждение.

2. Ответить для себя на следующие вопросы:

– ***Я ждал это письмо?***

– ***Я знаю отправителя?***

Если на один из вопросов был дан ответ **«Нет»**, то можно предположить, что это нежелательное письмо.

3. Проверить в письме наличие гиперссылки или вложения (файла).

4. Проверить гиперссылку на предмет подлога и web-подделки.

Первый способ: *Навести курсор мыши на ссылку в письме. В левом нижнем углу экрана браузера будет отображён адрес сайта, на который вас хотят перевести.*

Второй способ: *Нажать на ссылку правой кнопкой мыши, выбрать «копировать гиперссылку», откытый любой текстовый редактор (Р-7 офис, блокнот и т. д.) и вставить скопированный текст.*

Если ссылка из вашего письма и та, которую вы увидите после проверки, будут отличаться, письмо прислали мошенники и открывать ссылку опасно.

Помните, что фишинговые письма могут содержать веб-адрес, визуально похожий на настоящий адрес сайта, однако в ссылке может скрываться намеренная опечатка, например, «I» может быть заменена на «1». Такая ссылка будет вести на фальшивый сайт, который создали мошенники.

Внимательно проверяйте гиперссылки, даже если письмо получено от отправителя, которого вы знаете.

5. Читайте внимательно письмо, орфографические, грамматические или пунктуационные ошибки могут быть признаками фишингового письма (рис. 5).

Среди злоумышленников нередко встречаются малограмотные личности или те, кто вовсе не говорит на русском языке, а текст сообщения набирает с помощью онлайн-переводчика.

6. Обращайте внимание на детали письма, даты, места и другие нюансы, которые помогут понять, что данное письмо не имеет к вам никакого отношения.

Обычно злоумышленники пытаются сделать свои письма предельно нейтральными, чтобы минимизировать количество признаков, по которым можно отличить фальшивое сообщение от настоящего.

7. Вас должно насторожить, если тема, содержание письма или название файлов побуждают к немедленному действию (к переходу по ссылке, к нажатию на кнопку, к открытию файла, к немедленному ответу на письмо) либо вызывают у тебя любопытство.

Мошенники – хорошие психологи, и они используют любые способы, чтобы убедить жертву открыть ссылку или скачать вложение.

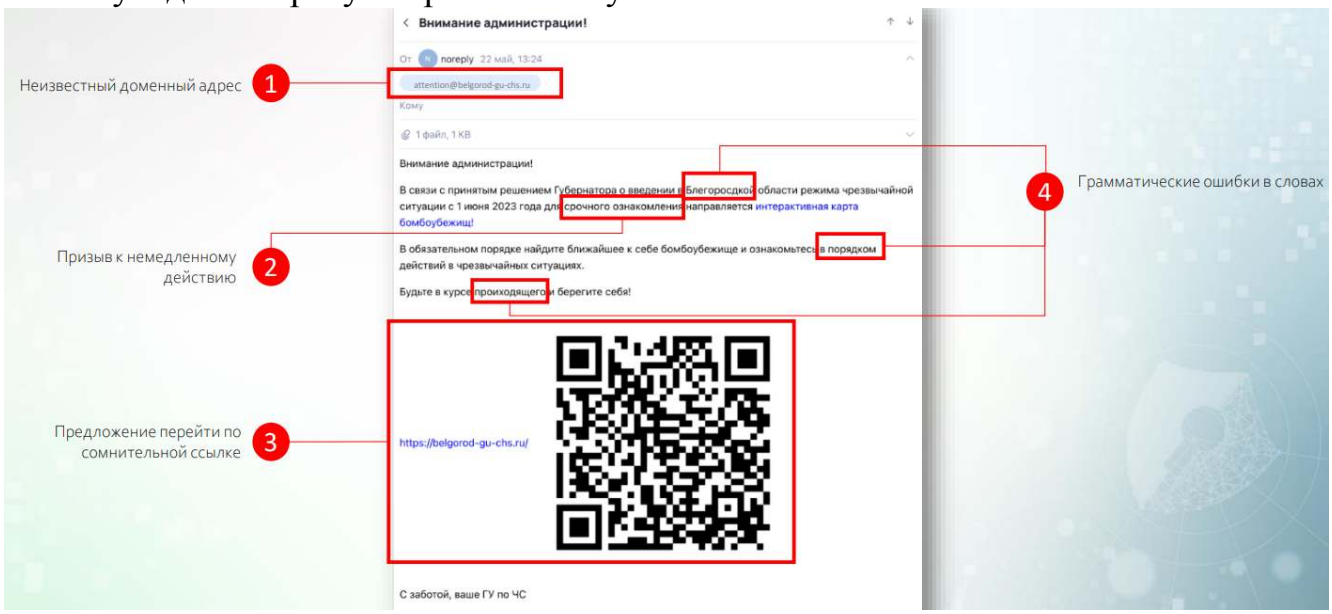

Рис. 5 Признаки фишингового письма.

Если письмо выглядит правдоподобно, но вы всё равно сомневаетесь, не стесняйтесь обратиться за помощью к руководителю или ответственному за защиту информации.

Что делать, если вы перешли по фишинговой ссылке?

1. Не вводить данные от учётных записей.

2. Не совершать никаких действий на сайте и как можно скорее закрыть ссылку.

3. Проверить устройство антивирусом, чтобы убедиться, что при переходе по ссылке не были скачаны сторонние файлы.

4. В случае, если вы всё-таки попались на уловку злоумышленников, **не паникуйте** и как можно скорее сообщите об этом руководителю и сотруднику, ответственному за защиту информации.

5. **Если Вы всё-таки ввели свои учётные данные, то как можно быстрее необходимо изменить пароль!**

6. Если вы ждали письмо, но сомневаетесь в легитимности информации изложенной в нём, необходимо связаться с отправителем по контактам, отличным от оставленных в письме.

7. Подозрительные письма и сообщения необходимо пересылать на адрес электронной почты **AVZ@BELREGION.RU**

8. В процессе работы пользователю автоматизированного рабочего места запрещается:

– оставлять без личного контроля свой персональный идентификатор, пароль и передавать его другим лицам;

– использовать недокументированные свойства и ошибки в программном обеспечении или в настройках технических средств, которые могут привести к возникновению нештатных ситуаций;

– самостоятельно и без разрешения ответственного за защиту информации вносить изменения в состав, конструкцию, конфигурацию и изменять места расположения технических средств АРМ;

– производить модификацию, уничтожение и блокирование в отношении общего и специального (прикладного) программного обеспечения, применяемого для обработки информации;

– осуществлять попытки несанкционированного доступа к информационным ресурсам АРМ;

– отключать (блокировать) средства защиты информации АРМ;

– использовать неисправные машинные носители информации (далее– МНИ) для её хранения и обработки;

– использовать неучтённые МНИ;

– разглашать сведения о реализованном на АРМ комплексе средств защиты информации (антивирусные средства, криптографической защиты и т. п.);

– оставлять АРМ при выходе из помещения, в котором оно установлено, не убедившись, что оно заблокировано или отключено.

<u>Важно знать</u> – информация, составляющая государственную тайну, и иные сведения, которые могут нанести ущерб безопасности Российской Федерации, обрабатываются в специальных помещениях на специальных аттестованных АРМ (аттестованных объектах информатизации).

9. Сотрудник обязан:

– немедленно докладывать руководителю и ответственному за защиту информации о выявленных изменениях в конфигурации технических средств и программного обеспечения АРМ;

– сообщать руководителю и ответственному за защиту информации о фактах и попытках несанкционированного доступа к обрабатываемой

информации на АРМ.

Незамедлительно информировать руководителя и ответственного за защиту информации **о возникновении нештатных ситуаций, связанных с использованием АРМ, таких как:**

– подозрения в компрометации (разглашении, утечке, несанкционированном копировании или использовании) личных паролей или закрытых ключей, применяемых для входа в АРМ;

– подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках);

– несанкционированные изменения в конфигурации программных или аппаратных средств (произведённых с нарушением установленного порядка);

– отклонения в нормальной работе системного и прикладного программного обеспечения, затрудняющие эксплуатацию автоматизированного рабочего места;

– обнаружение ошибок в программном обеспечении или в настройках технических средств АРМ;

– некорректное функционирование установленных в АРМ средств защиты информации;

– несоблюдение требований инструкций по защите информации.

ВАЖНО ЗАПОМНИТЬ!!!

При возникновении проблем, связанных с эксплуатацией АРМ, таких как неисправная работа периферийных устройств, организационной техники (мышь, клавиатура, монитор, системный блок, принтер, МФУ, сетевое подключение и т. п.), при сбоях в работе операционной системы, программного обеспечения, возникновении ошибок авторизации и иных отклонениях в нормальной работе АРМ сотрудник обязан уведомить об этом руководителя структурного подразделения и ответственного за защиту информации, подать заявку в службу поддержки для устранения выявленных недостатков.

Не пытайтесь решить проблему самостоятельно (осуществить ремонт или настройку АРМ)!!! *Это запрещено и влечёт персональную ответственность сотрудника в соответствии с действующим законодательством Российской Федерации*.

10. Ответственность за неисполнение данных требований:

Сотрудник несёт персональную ответственность за ненадлежащее исполнение своих обязанностей, а также сохранность комплекта АРМ, МНИ, электронных идентификаторов и целостность установленного программного обеспечения.

Ответственность за нарушение функционирования АРМ или его компонентов, уничтожение, блокирование, несанкционированные операции копирования и распространения, а также модификации и замены информации,

обрабатываемой на АРМ, несёт сотрудник, идентификационные данные которого были использованы при совершении нарушения.

Сотрудники, виновные в нарушениях, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Уголовным кодексом Российской Федерации статьёй 274. «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» предусмотрена ответственность за нарушения:

1. Штраф в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осуждённого за период до восемнадцати месяцев, либо исправительные работы на срок от шести месяцев до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо лишение свободы на тот же срок.

2. Принудительные работы на срок до пяти лет либо лишение свободы на тот же срок.

Уголовным кодексом Российской Федерации статьёй 272. «Неправомерный доступ к компьютерной информации» предусмотрена ответственность за следующие нарушения:

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осуждённого за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершённое из корыстной заинтересованности, наказывается штрафом в размере от ста тысяч до трёхсот тысяч рублей или в размере заработной платы или иного дохода осуждённого за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырёх лет, либо принудительными работами на срок до четырёх лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй статьи 272, совершённые группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трёх лет с лишением права занимать определённые должности или заниматься определённой деятельностью на срок до трёх лет, либо ограничением свободы на срок до четырёх лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей статьи 272, если они повлекли тяжкие последствия или создали угрозу их наступления, наказываются лишением свободы на срок до семи лет.

Также предусмотрено наказание в соответствии с Кодексом Российской Федерации об административных правонарушениях.

Статья 13.14 Кодекса Российской Федерации об административных правонарушениях.

Разглашение информации с ограниченным доступом влечёт наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц – от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трёх лет; на юридических лиц – от ста тысяч до двухсот тысяч рублей.

Статья 13.14.1 Кодекса Российской Федерации об административных правонарушениях.

Незаконное получение информации с ограниченным доступом влечёт наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц – от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трёх лет; на юридических лиц – от ста тысяч до двухсот тысяч рублей.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 00aad08de24d589fabbd257ae4d06803a6
Владелец Мирошников Евгений Владимирович
Действителен с 17.04.2023 по 10.07.2024

Первый заместитель Губернатора области – министр цифрового развития области **Е.В. Мирошников**