ГЛАВА АДМИНИСТРАЦИИ ОКТЯБРЬСКОГО РАЙОНА ГОРОДА ПЕНЗЫ

ПРИКАЗ

от 25 октября 2021 г. N 341

ОБ УТВЕРЖДЕНИИ РЕГЛАМЕНТА РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ

ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫЕ

С СОВЕРШЕНИЕМ КОМПЬЮТЕРНЫХ АТАК, ВНЕДРЕНИЕМ ВРЕДОНОСНОГО

ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ТАКЖЕ ВОЗМОЖНЫМИ ТЕХНИЧЕСКИМИ

СБОЯМИ В РАБОТЕ И ПРАВИЛ ПО БЕЗОПАСНОЙ РАБОТЕ

ПРИ ОСУЩЕСТВЛЕНИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

"ИНТЕРНЕТ"

Руководствуясь Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", приказываю:

1. Утвердить прилагаемые:

1.1. [Регламент](#P41) реагирования на компьютерные инциденты информационной безопасности, связанные с совершением компьютерных атак, внедрением вредоносного программного обеспечения, а также возможными техническими сбоями в работе.

1.2. [Правила](#P171) по безопасной работе при осуществлении информационного взаимодействия с использованием информационно-телекоммуникационной сети "Интернет".

1.3. [Правила](#P359) выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации, и реагирования на них.

1.4. [Порядок](#P496) защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

1.5. [Политику](#P523) в отношении обработки и защиты персональных данных.

1.6. [Порядок](#P587) обезличивания персональных данных граждан и работников администрации Октябрьского района города Пензы, правила работы с обезличенными персональными данными.

2. Настоящий приказ действует в части, не противоречащей законодательству, регулирующему отношения связанные с обработкой персональных данных, осуществляемой органами местного самоуправления.

3. Настоящий приказ опубликовать в муниципальной газете "Пенза" и разместить на интернет-странице администрации Октябрьского района города Пензы официального сайта администрации города Пензы в информационно-телекоммуникационной сети "Интернет".

4. Контроль за выполнением настоящего приказа возложить на заместителя главы администрации Октябрьского района города Пензы по организации деятельности администрации района.

Глава администрации

А.В.ГРИШИН

Утвержден

приказом

главы администрации

Октябрьского района

города Пензы

от 25 октября 2021 г. N 341

РЕГЛАМЕНТ

РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ

БЕЗОПАСНОСТИ, СВЯЗАННЫЕ С СОВЕРШЕНИЕМ КОМПЬЮТЕРНЫХ АТАК,

ВНЕДРЕНИЕМ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ТАКЖЕ

ВОЗМОЖНЫМИ ТЕХНИЧЕСКИМИ СБОЯМИ В РАБОТЕ

1. Термины и определения

В настоящем Регламенте используются следующие термины:

Информационная безопасность (далее - ИБ) - это процесс обеспечения конфиденциальности, целостности и доступности информации.

Событие информационной безопасности - нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Инцидент информационной безопасности (далее - инцидент ИБ) - событие в информационной системе, ставящее под угрозу защиту информации.

Администратор ИБ - заместитель начальника отдела делопроизводства и хозяйственного обеспечения администрации района. Отвечает за организацию защиты информации локальной сети администрации Октябрьского района города Пензы.

Пользователь - сотрудник администрации Октябрьского района города Пензы.

Автоматизированное рабочее место (далее - АРМ) - рабочее место пользователя (компьютер) для подготовки, редактирования, поиска и выдачи на экран и печати необходимых ему документов и данных.

2. Общие положения

Целью Регламента является обеспечение своевременного реагирования и оповещения об инцидентах ИБ при повседневной работе администрации Октябрьского района города Пензы.

Пользователь и администратор ИБ в своей работе руководствуются следующими федеральными законами: от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и защите информации", от 27.07.2006 N 152-ФЗ "О персональных данных", от 06.04.2011 N 63-ФЗ "Об электронной подписи", приказами Федеральной службы по техническому и экспортному контролю от 18.02.2013 N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", настоящим Регламентом и иными документами в области информационной безопасности.

3. События информационной безопасности, приводящие

к возникновению инцидентов информационной безопасности

Событиями информационной безопасности, приводящими к инцидентам ИБ, могут являться:

- появление файлов с нетипичным именем, форматом или большим размером;

- исчезновение файлов или папок;

- модификация файлов или их содержимого;

- выполнение процессов, не запускаемых пользователем;

- значительное замедление работы программного обеспечения;

- резкое сокращение свободного пространства на жестком диске;

- блокировка экрана монитора или средств ввода/вывода информации;

- появление рекламных или иных баннеров на экране монитора;

- самопроизвольное скачивание и/или запуск/установка файлов;

- изменение/блокировка учетных данных пользователя или доступа к ресурсам;

- умышленные действия пользователя, включающие самовольную установку системного и/или программного обеспечения, а также иные действия, приводящие к техническим сбоям в работе компьютерного оборудования;

- другие события, которые могут привести к несанкционированному доступу к ресурсам или отказу в обслуживании.

4. Первоочередные меры при обнаружении инцидента

информационной безопасности, связанного с совершением

компьютерных атак и внедрением вредоносного программного

обеспечения

Инцидентом ИБ, связанным с совершением компьютерных атак и внедрением вредоносного программного обеспечения, необходимо считать состояние системы, которое привело к несанкционированному доступу к служебной информации и/или ресурсам администрации города Пензы.

При наступлении инцидента ИБ пользователю необходимо незамедлительно обратится к администратору ИБ.

Основными первоочередными мерами по нейтрализации последствий инцидентов ИБ, связанных с совершением компьютерных атак и внедрением вредоносного программного обеспечения, являются:

- отключение АРМ сотрудника от локальной сети администрации района (производится незамедлительно при обнаружении события ИБ, приводящего к возникновению инцидента ИБ);

- отключение АРМ сотрудника от информационно-телекоммуникационной сети "Интернет" (производится незамедлительно при обнаружении события ИБ, приводящего к возникновению инцидента ИБ);

- незамедлительное оповещение администратора ИБ;

- незамедлительное отключение питания компьютера (при отключении питания компьютера не пытаться его перезагрузить или включить заново, так как эти действия приводят к изменению файловой системы);

- подготовка докладной записки на имя заместителя главы администрации района по организации деятельности администрации, отражающей последовательность действий, приведших к наступлению инцидента ИБ;

- внесение записи администратором ИБ в [журнал](#P124) инцидентов ИБ приведенный в приложении к настоящему Регламенту.

5. Действия при наступлении инцидентов

информационной безопасности

5.1. Обязанности пользователя:

5.1.1. Соблюдать требования Правил по безопасной работе осуществлении организации информационного взаимодействия с использованием информационно-телекоммуникационной сети "Интернет" (далее - Правила).

5.1.2. Выполнять требования и рекомендации администратора информационной безопасности, соблюдения политики информационной безопасности администрации Октябрьского района города Пензы.

5.1.3. При обнаружении событий, указанных в [разделе 3](#P62) настоящего Регламента, незамедлительно информировании администратора ИБ города администрации Октябрьского района города Пензы.

5.2. Обязанности администратора ИБ:

5.2.1. Проводить периодический (первичный и повторный не реже одного раза в год) инструктаж пользователей по вопросу информационной безопасности согласно Правилам, настоящему Регламенту и действующему законодательству по защите информации. Отметки о проведении инструктажа заносить в журнал регистрации инструктажей и заверять собственноручной подписью инструктируемого участника взаимодействия.

5.2.2. Контролировать соблюдение пользователями Правил.

5.2.3. Информировать заместителя главы администрации района по организации деятельности администрации о фактах нарушений требований Правил со стороны пользователей.

5.2.4. Обеспечивать функционирование установленных средств защиты информации.

5.2.5. Своевременно информировать руководство об истечении срока действия сертификатов соответствия на средства защиты информации.

5.2.6. Вести [журнал](#P124) инцидентов информационной безопасности, приведенный в Приложении к настоящему Регламенту.

Приложение

к Регламенту

реагирования на компьютерные

инциденты информационной

безопасности, связанные

с совершением компьютерных атак,

внедрением вредоносного

программного обеспечения,

а также возможными техническими

сбоями в работе

ФОРМА ЖУРНАЛА

инцидентов информационной безопасности

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| N п/п | Дата и время обнаружения инцидента ИБ | Кем обнаружен инцидент ИБ (ФИО, должность) | Описание инцидента ИБ | Способ решения инцидента ИБ | Дата и время решения проблемы | Отметка о доведении в УИ ПО (дата, время, кто принял информацию) | Подпись администратора информационной безопасности |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Утверждены

приказом

главы администрации

Октябрьского района

города Пензы

от 25 октября 2021 г. N 341

ПРАВИЛА

ПО БЕЗОПАСНОЙ РАБОТЕ ПРИ ОСУЩЕСТВЛЕНИИ ИНФОРМАЦИОННОГО

ВЗАИМОДЕЙСТВИЯ С ИСПОЛЬЗОВАНИЕМ

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ"

1. Термины и определения

В настоящих Правилах используются следующие термины и определения:

Автоматизированное рабочее место (далее АРМ) - рабочее место пользователя (компьютер) для подготовки, редактирования, поиска и выдачи на экран и печати необходимых ему документов и данных.

Пользователь - сотрудник администрации района.

Антивирусное программное обеспечение - специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления зараженных (модифицированных) такими программами файлов, а также профилактики заражения (модификации) файлов или операционной системы вредоносным кодом.

Резервное копирование - процесс создания копии данных на носителе (жестком диске, дискете, флэш-накопителе), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Вредоносный объект - программное обеспечение, позволяющее получить несанкционированный доступ к вычислительным ресурсам ЭВМ, а также данным, которые на ней хранятся.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

Электронная подпись - уникальный цифровой код, который используется для подписания документа в электронной форме, и позволяет идентифицировать лицо, подписавшее документ.

Администратор ИБ - заместитель начальника отдела делопроизводства и хозяйственного обеспечения администрации района. Отвечает за организацию защиты информации локальной сети администрации.

Мессенджер-программа, мобильное приложение или веб-сервис для мгновенного обмена сообщениями.

Иностранные Интернет-приложения - зарубежные прикладные компьютерные приложения, предоставляющие в информационно-телекоммуникационной сети "Интернет" возможности электронной почты, системы обмена мгновенными сообщениями, голосовой и видеоинформацией, социальных сетей, облачных сервисов.

Аутентификационные данные - логин, пароль либо иная информация, используемая для идентификации пользователя.

Компрометация аутентификационных данных - утрата доверия к тому, что используемые аутентификационные данные обеспечивают безопасность информации (утрата, разглашение, кража, взлом).

2. Общие положения

Настоящие Правила разработаны в соответствии с Федеральными законами от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и защите информации", от 27.07.2004 N 152-ФЗ "О персональных данных", от 06.04.2011 N 63-ФЗ "Об электронной подписи", приказами Федеральной службы по техническому и экспортному контролю от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", от 11.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", совместным приказом Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю от 31.08.2010 N 416/N 489 "Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования" и иными нормативными документами в области информационной безопасности.

Пользователь в своей работе руководствуется Правилами, а также иными руководящими, нормативными и регламентирующими документами в области информационной безопасности.

3. Правила безопасности при осуществлении информационного

взаимодействия

3.1. обеспечивает пользователям АРМ с предустановленным лицензионным системным и прикладным программным обеспечением (на котором обеспечивается своевременная установка обновлений системы безопасности). Дополнительная установка программ, параметров и компонентов производится только по поручению администратора ИБ. При привлечении посторонних лиц для ремонта или настройки АРМ необходимо присутствие администратора ИБ, либо сотрудника его заменяющего.

3.2. Администрация Октябрьского района города Пензы обеспечивает наличие сертифицированных по требованиям безопасности информации межсетевых экранов для каждой точки подключения к информационно-телекоммуникационной сети "Интернет".

3.3. Порядок выполнения регулярного резервного копирования личных файлов и параметров АРМ пользователей определяется администратором ИБ.

3.4. Порядок использования электронной подписи осуществляется в соответствии с [Руководством](#P261) по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, выданным Удостоверяющим центром Управления Федерального казначейства по Пензенской области.

3.5. При эксплуатации АРМ и информационных систем запрещается:

- использование доступа к информационно-телекоммуникационной сети "Интернет" в личных целях;

- посещение досугово-развлекательных сайтов (игровые сайты, интернет-магазины, сайты "для взрослых", онлайн-кинотеатры);

- распространение и тиражирование информации, служебной информации и информации, за распространение которой предусмотрена уголовная или административная ответственность;

- отключение (блокировка) средств защиты информации;

- подключение к АРМ и локальной вычислительной сети посторонних и личных устройств (смартфонов, телефонов, USB-накопителей информации, считывателей карт памяти, карт памяти, модемов, роутеров, устройств с модулями Bluetooth);

- передача аутентификационных данных посторонним лицам (пароли, логины, ключи электронной цифровой подписи) При компрометации аутентификационных данных необходимо сразу сообщить администратору ИБ;

- использование личной электронной почты на АРМ в служебных целях (личным считается почтовый ящик, не согласованный с администрацией района);

- скачивание, открытие файлов и запуск программ, полученных из непроверенных источников;

- использование мессенджеров для обмена служебной информацией без согласования с администрацией района.

3.6. При эксплуатации АРМ и информационных систем в администрации Октябрьского района города Пензы необходимо выполнять следующие правила:

- соблюдать Инструкцию Пользователя;

- при выборе пароля для создания учетных записей соблюдать требования формирования паролей;

- при вынужденном отсутствии на рабочем месте осуществлять блокировку АРМ или выход из учетной записи;

- администратору ИБ регулярно обновлять антивирусные базы (при возможности настройки антивирусного средства - автоматическое обновление или в ручном режиме - не реже одного раза в три дня);

- администратору ИБ проводить полную профилактическую проверку АРМ пользователя антивирусным программным обеспечением на присутствие вредоносных объектов не реже одного раза в квартал;

- перед открытием файлов, скачанных из информационно-телекоммуникационной сети "Интернет", осуществлять их проверку антивирусным программным обеспечением на наличие вредоносного кода;

- при получении подозрительного письма на адрес электронной почты от неизвестного адресата проконсультироваться с администратором ИБ;

- не устанавливать и не использовать в служебных целях иностранные интернет-сервисы.

3.7. При обнаружении событий информационной безопасности, приводящих к инцидентам информационной безопасности, следовать действиям согласно Регламенту реагирования на компьютерные инциденты информационной безопасности, связанные с совершением компьютерных атак, внедрением вредоносного программного обеспечения, а также возможными техническими сбоями в работе.

4. Формирование паролей

4.1. При формировании пароля рекомендуется использовать символы трех категорий из числа категорий, приведенных ниже:

- прописные буквы латинского алфавита от А до Я;

- строчные буквы латинского алфавита от а до я;

- цифры (от 0 до 9);

- символы, не принадлежащие алфавитно-цифровому набору (например: @, !, $, #, %).

4.2. В соответствии с Правилами запрещается:

- использовать пароль, состоящий менее чем из шести символов;

- использовать в качестве пароля имя учетной записи пользователя или какую-либо его часть;

- включать в пароль легко вычисляемые сочетания символов, простые пароли типа "123", "111", "qwerty" и им подобные, а также ФИО и даты рождения свою и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые могут быть подобраны, основываясь на информации о пользователе;

- использовать в качестве пароля один и тот же повторяющийся символ, либо повторяющуюся комбинацию из нескольких символов (например, "222222");

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

использовать ранее использованные пароли;

- использовать один пароль в разных информационных ресурсах.

5. Правила пользования государственными и муниципальными

информационными системами

5.1. АРМ, используемые для работы с государственными и муниципальными информационными системами (далее - ГИС и МИС), должны соответствовать требованиям, изложенным в документации соответствующих ГИС и МИС.

5.2. Перед началом работы в ГИС и МИС пользователи должны ознакомиться с правилами работы в соответствующих ГИС и МИС (инструкциями пользователей).

5.3. Контроль защищенности эксплуатируемых информационных систем осуществляется администратором ИБ не реже одного раза в квартал.

Приложение

к Правилам

по безопасной работе при

осуществлении информационного

взаимодействия с использованием

информационно-

телекоммуникационной сети

"Интернет"

РУКОВОДСТВО

ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ КВАЛИФИЦИРОВАННОЙ

ЭЛЕКТРОННОЙ ПОДПИСИ И СРЕДСТВ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ

ПОДПИСИ

1. Общие положения

Настоящее Руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 N 63-ФЗ "Об электронной подписи" и является средством официального информирования лиц, заинтересованных в получении или владеющих квалифицированной электронной подписью, об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

Применение квалифицированной электронной подписи в системах юридически значимого электронного документооборота и иных системах сопровождается рисками финансовых убытков и иного рода потерь, связанных с признанием недействительности сделок, совершенных с использованием квалифицированной электронной подписи при несанкционированном получении злоумышленником ключа электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка квалифицированной электронной подписи. В связи с этим необходимо выполнение приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

2. Требования по размещению

При размещении средств квалифицированной электронной подписи:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной электронной подписи, посторонних лиц, не имеющих допуск к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3. Требования по установке средств квалифицированной

электронной подписи, общесистемного и специального

программного обеспечения

При использовании средств квалифицированной электронной подписи должны выполняться следующие меры по защите информации от несанкционированного доступа:

3.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем и нижнем регистрах, цифры и специальные символы (@, !, $, #, %);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения) а также сокращения (USER, ADMIN, root);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- личный пароль пользователь не имеет права никому сообщать;

- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

3.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

- не использовать нестандартные, измененные или отладочные версии операционных систем;

- исключить возможность загрузки и исполнения операционной, системы, отличной от предусмотренной штатной работой;

- исключить возможность удаленного управления, администрирования и модификации операционной систем и ее настроек;

- на средствах вычислительной техники с установленными средствами квалифицированной электронной подписи должна быть установлена только одна операционная система;

- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы);

- режимы безопасности, реализованные в операционной системе, быть настроены на максимальный уровень;

- всем пользователям и группам, зарегистрированным в операционной системе, системе, необходимо назначить максимально возможные для работы права;

3.3. Необходимо предусмотреть меры, максимально ограничивающие доступ к:

- ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части);

- системному реестру;

- файлам и каталогам;

- временным файлам;

- журналам системы;

- файлам подкачки;

- кэшируемой информации (пароли);

- отладочной информации.

Кроме того, необходимо организовать стирание (по окончании сеанса работы средств квалифицированной электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

Должно быть исключено попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий.

Необходимо регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.

В случае подключения технических средств с установленными средствами квалифицированной электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем к программному обеспечению, в окружении которого функционируют средства квалифицированной электронной подписи, и к компонентам средств квалифицированной электронной подписи со стороны указанных сетей должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей). Все средства защиты должны иметь сертификат уполномоченного органа по сертификации средств защиты.

3.4. Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.

3.5. Организовать и использовать комплекс мероприятий по антивирусной защите.

Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;

использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

- вносить какие-либо изменения в программное обеспечение средств;

- работать со средствами квалифицированной электронной подписи при включенных в техническое средство штатных средствах входа в радиоканал;

- записывать на ключевые носители постороннюю информацию;

- оставлять средства вычислительной техники с установленными средствами квалифицированной электронной подписи без контроля после ввода ключевой информации.

3. Требования по обеспечению информационной безопасности

при обращении с носителями ключевой информации, содержащими

ключи квалифицированной электронной подписи

4.1. Меры защиты ключей квалифицированной электронной подписи. Ключи квалифицированной электронной подписи при их создании должны записываться на типы ключевых носителей, которые поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

Ключи квалифицированной электронной подписи могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной электронной подписи.

Если процедуру генерации ключей выполняет сотрудник Удостоверяющего центра, то он должен сообщить сформированный пароль (ПИН-код) владельцу ключа квалифицированной электронной подписи.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

4.2. Обращение с ключевой информацией и ключевыми носителями. Недопустимо пересылать файлы с ключевой информацией для работы в системах обмена электронными документами по электронной почте сети "Интернет" или по внутренней электронной почте (кроме запросов на сертификат и открытых ключей).

Ключевая информация должна размещаться на сменном носителе информации (floppy-диск, USB-flash-накопитель, e-Token, ru-Token)/Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем либо Уполномоченным лицом на использование данного носителя и храниться в месте, не доступном третьим лицам (сейф, опечатанный бокс, закрывающийся металлический шкаф).

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

4.3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи.

С целью контроля исходящего и входящего подозрительного трафика технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку в "Интернет" информации, инициированную программами, не имеющими соответствующих полномочий.

На технических средствах, используемых для работы в системах обмена электронными документами:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в [разделе 3](#P277) Руководства;

- должно быть установлено только лицензионное программное обеспечение;

- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;

- должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в том числе службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски);

- должны регулярно устанавливаться обновления операционной системы;

- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной электронной подписи, и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в системе обмена электронными документами;

- должна быть активирована подсистема регистрации событий информационной безопасности;

- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В качестве автоматизированного рабочего места для работы в системах обмена электронными документами не рекомендуется выбирать переносной компьютер (ноутбук). Если выбран ноутбук, недопустимо его подключение к сетям общего доступа в местах свободного доступа в "Интернет" (интернет-кафе, гостиницы, офисные центры), при этом для хранения ключевой информации должен использоваться сменный носитель информации.

В случае передачи (списания технических средств, на которых были установлены ключи квалифицированной электронной подписи, необходимо гарантированно удалять всю информацию, использование которой третьими лицами может потенциально нанести вред организации, в том числе средства квалифицированной электронной подписи, журналы работы систем обмена электронными документами.

Утверждены

приказом

главы администрации

Октябрьского района

города Пензы

от 25 октября 2021 г. N 341

ПРАВИЛА

ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ, КОТОРЫЕ МОГУТ ПРИВЕСТИ К СБОЯМ ИЛИ

НАРУШЕНИЮ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ И (ИЛИ)

К ВОЗНИКНОВЕНИЮ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ,

И РЕАГИРОВАНИЯ НА НИХ

1. Термины и определения

Информационная безопасность (далее - ИБ) - процесс обеспечения конфиденциальности, целостности и доступности информации.

Событие информационной безопасности - идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Инцидент - одно событие или группы событий, которые могут привести к сбоям или нарушению функционирования информационной системы (далее - ИС) и (или) к возникновению угроз безопасности, в том числе персональных данных.

2. Общие положения

Настоящие Правила разработаны в соответствии с Федеральным законом N 152-ФЗ "О персональных данных", Федеральным законом N 149-ФЗ "Об информации, информационных технологиях и о защите информации", постановлением Правительства РФ N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказом ФСТЭК России N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", Распоряжением Правительства Пензенской области от 7 июня 2017 года N 261-рП "Об утверждении Регламента реагирования на компьютерные инциденты, связанные с совершением компьютерных атак, внедрением вредоносного программного обеспечения, а также возможными техническими сбоями в работе и Свода правил по безопасной работе при осуществлении информационного взаимодействия с использованием информационно-телекоммуникационной сети "Интернет", Политикой в отношении обработки и защиты персональных данных в администрации Октябрьского района города Пензы.

Работа с инцидентами включает в себя следующие направления:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;

- обнаружение, идентификация и регистрация инцидентов;

- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

- принятие мер по устранению последствий инцидентов;

- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

Полномочия по анализу инцидентов, в том числе определению источников и причин возникновения инцидентов, а также оценке их последствий; планированию и принятию мер по предотвращению повторного возникновения инцидентов, возлагаются на постоянно действующую комиссию по защите персональных данных, состав которой утверждается приказом главы администрации Октябрьского района города Пензы.

3. Ответственные за выявление инцидентов и реагирование

на них

3.1. В информационных системах.

3.1.1. Ответственными за выявление инцидентов в ИС являются:

- лица, имеющие право доступа к ИС;

- ответственный за техническую защиту информации в ИСПДн администрации района;

- администратор ИС;

- администратор информационной безопасности ИС.

3.1.2. Ответственными за реагирование на инциденты в ИС являются:

- лица, имеющие право доступа к ИС;

- начальник отдела администрации, в котором выявлен инцидент;

- ответственный за техническую защиту информации в ИСПДн администрации района;

- администратор ИС;

- администратор информационной безопасности ИС;

- ответственный за организацию обработки персональных данных администрации района, в случае, если ИС является информационной системой персональных данных (далее - ИСПДн);

- председатель постоянно действующей комиссии по защите персональных данных.

3.2. Вне информационных систем.

3.2.1. Ответственными за выявление инцидентов вне ИС являются все сотрудники администрации Октябрьского района города Пензы.

3.3. Ответственными за реагирование на инциденты вне ИС являются:

- сотрудник администрации района, обнаруживший инцидент;

- начальник отдела администрации района, в котором выявлен инцидент;

- ответственный за организацию обработки персональных данных администрации района, в случае, если существует угроза безопасности персональных данных;

- председатель постоянно действующей комиссии по защите персональных данных.

4. Обнаружение, идентификация и регистрация инцидентов

4.1. Работа по обнаружению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

- выявление инцидентов в области информационной безопасности с помощью технических средств;

- выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;

- выявление инцидентов с помощью сотрудников администрации района.

4.2. Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на доведение до сотрудников администрации района информации, позволяющей идентифицировать инциденты.

4.3. Регистрация инцидентов осуществляется в журнале регистрации инцидентов информационной безопасности. Форма [журнала](#P457) утверждается главой администрации Октябрьского района города Пензы (приложение).

5. Информирование о возникновении инцидентов

5.1. Сотрудник администрации (пользователь), обнаруживший инцидент в ИС, должен незамедлительно сообщить об инциденте начальнику отдела, администратору ИС, администратору информационной безопасности ИС, ответственному за организацию обработки персональных данных (в случае если ИС является ИСПДн), председателю постоянно действующей комиссии защите персональных данных.

5.2. Администратор ИС, в случае необходимости, информирует пользователей ИС о возникновении инцидента и дает указания по дальнейшим действиям.

6. Анализ инцидентов, а также оценка их последствий

6.1. Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий осуществляет постоянно действующая комиссия по защите персональных данных.

6.2. Оценка последствий инцидента производится на основании потенциально возможного ущерба.

7. Принятие мер по устранению последствий инцидентов

Меры по устранению последствий инцидентов включает в себя мероприятия, направленные на:

- определение границ инцидента и ущерба от реализации угроз информационной безопасности;

- ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

7. Планирование и принятие мер по предотвращению инцидентов

Планирование и принятие мер по предотвращению повторного возникновения инцидентов осуществляет постоянно действующая комиссия по защите персональных данных и основывается на:

- планомерной деятельности по повышению уровня информационной безопасности при работе в ИСПДн администрации района;

- проведении мероприятий по обучению сотрудников администрации района правилам и способам работы со средствами защиты информационных систем;

- доведении до сотрудников норм законодательства, внутренних документов администрации района, устанавливающих ответственность за нарушение требований информационной безопасности;

- разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимаемыми на работу;

- своевременной модернизации системы обеспечения информационной безопасности с учетом возникновения новых угроз информационной безопасности;

- своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

Приложение

к Правилам

выявления инцидентов, которые

могут привести к сбоям или

нарушению функционирования

информационной системы и (или)

к возникновению угроз

безопасности информации,

и реагирования на них

ФОРМА ЖУРНАЛА

инцидентов информационной безопасности

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| N п/п | Дата и время обнаружения Инцидента ИБ | Кем обнаружен Инцидент ИБ (ФИО, должность) | Описание инцидента ИБ | Способ решения инцидента ИБ | Дата и время решения проблемы | Отметка об уведомлении начальника Управления информационных технологий и связи Пензенской области | Подпись администратора информационной безопасности |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Утвержден

приказом

главы администрации

Октябрьского района

города Пензы

от 25 октября 2021 г. N 341

ПОРЯДОК

ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЫВОДЕ ИЗ ЭКСПЛУАТАЦИИ ИНФОРМАЦИОННОЙ

СИСТЕМЫ ИЛИ ПОСЛЕ ПРИНЯТИЯ РЕШЕНИЯ ОБ ОКОНЧАНИИ ОБРАБОТКИ

ИНФОРМАЦИИ

Настоящий порядок защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации разработан на основании Федерального закона РФ от 27 июля 2006 г. N 152-ФЗ "О персональных данных", в соответствии с частью 1 "Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами", утвержденных постановлением Правительства РФ от 21 марта 2012 г. N 211, Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

1. Вывод из эксплуатации информационной системы персональных данных в администрации Октябрьского района города Пензы производится на основании акта работы постоянно действующей комиссии по защите персональных данных.

2. Обеспечение защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации осуществляется в соответствии документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации администрации Октябрьского района города Пензы, и в том числе включает:

- архивирование информации, содержащейся в информационной системе;

- уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

2.1. Архивирование информации, содержащейся в информационной системе, осуществляется при необходимости дальнейшего использования ее в деятельности администрации Октябрьского района города Пензы.

2.2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

2.3. Уничтожение носителей информации производится при выводе их из эксплуатации.

3. Уничтожение ПДн на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление ПДн, или программным удалением информации принятыми для конкретного типа носителя методами.

4. По окончании процедуры уничтожения ответственным за организацию обработки персональных данных в администрации Октябрьского района города Пензы составляется соответствующий акт об уничтожении документов и (или) носителей, содержащих ПДн.

Утверждена

приказом

главы администрации

Октябрьского района

города Пензы

от 25 октября 2021 г. N 341

ПОЛИТИКА

В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящая Политика является выдержками из Положения "Об обработке и защите персональных данных" и устанавливает порядок обработки персональных данных в Администрации Октябрьского района города Пензы. Обработка персональных данных субъектов персональных данных осуществляется исключительно с целью исполнения функций, возложенных на администрацию как иного органа местного самоуправления.

2. Состав персональных данных

2.1. В администрации Октябрьского района города Пензы согласно Положению об администрации обрабатываются следующие категории персональных данных:

- сведения, необходимые для исполнения функций как иного органа местного самоуправления, образуемого по территориальному принципу и обладающего собственными полномочиями по решению вопросов местного значения, установленных Уставом города Пензы;

- сведения, необходимые для оказания муниципальных услуг гражданам, зарегистрированным на территории района.

3. Передача персональных данных

3.1. Администрация Октябрьского района города Пензы как Оператор не предоставляет и не раскрывает сведения, содержащие персональные данные, третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральными законами.

По мотивированному запросу персональные данные без согласия субъекта персональных данных могут быть переданы:

- в судебные органы в связи с осуществлением правосудия;

- в органы государственной безопасности;

- в органы прокуратуры;

- в органы полиции;

- в следственные органы;

- в миграционную службу;

- в иные органы в случаях, установленных нормативными правовыми актами, обязательными для исполнения.

Работники администрации не отвечают на вопросы, связанные с передачей персональной данных по телефону или факсу.

4. Права субъектов персональных данных

4.1. Субъект персональных данных вправе требовать от Оператора (администрации Октябрьского района города Пензы) уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Для реализации вышеуказанных прав субъект персональных данных может в порядке установленном ст. 14 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", обратиться у Оператору с соответствующим запросом. Для выполнения таких запросов представителю Оператора может потребоваться установить Вашу личность и запросить дополнительную информацию.

Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных (Управление Роскомнадзора по Пензенской области: г. Пенза, ул. Карпинского, 12) или в судебном порядке.

В некоторых случаях (особенно если Вы хотите удалить Ваши персональные данные или прекратить их обработку) это может означать, что Оператор не сможет предоставлять Вам заявленные услуги.

Кроме того, действующее законодательство может устанавливать ограничения и другие условия, касающиеся упомянутых выше Ваших прав.

5. Меры по обеспечению защиты персональных данных

5.1. Администрация Октябрьского района города Пензы предпринимает необходимые организационные и технические меры по защите персональных данных. Принимаемые меры основаны на требованиях ст. 18.1, ст. 19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Постановлении Правительства Российской Федерации от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

В частности:

1) Назначены лица, ответственные за организацию обработки и обеспечение безопасности персональных данных.

2) Разработано и внедрено Положение о защите персональных данных.

3) Лица, ведущие обработку персональных данных, проинструктированы и ознакомлены с нормативными правовыми актами, регламентирующими порядок работы и защиты персональных данных.

4) Разграничены права доступа к обрабатываемым персональным данным.

5) Помимо вышеуказанных мер, осуществляются меры технического характера, направленные на:

- предотвращение несанкционированного доступа к системам, в которых хранятся персональные данные;

- резервирование и восстановление персональных данных работоспособности технических средств и программного обеспечения, средств защиты информации в информационных системах персональных данных модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

6. Гарантии конфиденциальности

6.1. Информация, относящаяся к персональным данным, ставшая известной в связи с осуществлением администрацией своей деятельности, а ее работниками своих должностных обязанностей, является конфиденциальной информацией и охраняется законом.

Работники и иные лица, получившие доступ к персональным данным, обрабатываемым в Администрации Октябрьского района города Пензы, предупреждены о возможной дисциплинарной, административной, гражданско-правовой или уголовной ответственности в случае нарушения норм и требований действующего законодательства, регулирующего правила обработки и защиты персональных данных.

Изменения настоящей Политики

Руководство Администрации Октябрьского района города Пензы может изменять настоящую Политику. В случае внесения в настоящую Политику существенных изменений, администрация Октябрьского района города Пензы разместит уведомление о таких изменениях в начале этого документа.

Утвержден

приказом

главы администрации

Октябрьского района

города Пензы

от 25 октября 2021 г. N 341

ПОРЯДОК

ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ГРАЖДАН И РАБОТНИКОВ

АДМИНИСТРАЦИИ ОКТЯБРЬСКОГО РАЙОНА ГОРОДА ПЕНЗЫ, ПРАВИЛА

РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

1. Общие положения

1.1. Настоящий Порядок разработан в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" (с изменениями), приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных".

1.2. Настоящие Правила определяют порядок обезличивания персональных данных и работы с ними.

2. Термины и определения

1. В соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" в настоящем Порядке используются следующие понятия:

- персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

- обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

3. Условия обезличивания

3.1. Обезличивание персональных данных проводится с целью снижения ущерба от разглашения защищаемых персональных данных.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;

- замена части сведений идентификаторами;

- понижение точности некоторых сведений (например, "Место жительства" может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только населенный пункт);

- деление сведений на части и обработка в разных информационных системах.

3.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

4. Порядок обезличивания персональных данных

4.1 Администрация района издает приказ о необходимости обезличивания персональных данных.

4.2 Лица, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

4.3. Обезличивание персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

5. Порядок работы с обезличенными персональными данными

5.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

5.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

5.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;

- антивирусной политики;

- правил работы со съемными носителями;

- правил резервного копирования;

- правил доступа в помещения, в которых ведется обработка персональных данных.

5.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;

- правил доступа в помещения, где они хранятся.