ПРОЕКТ

« » 2017 года

**Постановление №\_\_\_ /\_\_\_**

**О мерах по обеспечению безопасности обработки информации на автоматизированных рабочих местах администрации городского округа «Вуктыл»**

В целях обеспечения безопасности информации при ее обработке на автоматизированных рабочих местах в администрации городского округа«Вуктыл»:

1. Утвердить Парольную политику администрации городского округа«Вуктыл» согласно приложению № 1.
2. Утвердить Инструкцию по антивирусной защите информации на автоматизированных рабочих местах администрации городского округа«Вуктыл» согласно приложению № 2.
3. Утвердить Перечень базового (разрешенного) программного обеспечения для выполнения должностных обязанностей пользователей на автоматизированных рабочих местах администрации городского округа«Вуктыл» согласно приложению № 3.
4. Утвердить Регламент работы пользователей автоматизированных рабочих мест администрации городского округа«Вуктыл», подключенных к корпоративной сети передачи данных и информационно-телекоммуникационной сети «Интернет» согласно приложению № 4.
5. Начальникам отделов администрации городского округа «Вуктыл» ознакомить под роспись работников с настоящим постановлением.
6. Контроль за исполнением настоящего постановления возложить на начальника отдела информационных технологий администрации городского округа «Вуктыл» Ротару К.В.

Руководитель администрации

городского округа«Вуктыл» В.Н. Крисанов

УТВЕРЖДЕНА

постановлением администрации

городского округа «Вуктыл»

от « \_\_\_» \_\_\_\_\_\_\_\_2017 г. № \_\_\_\_\_

(приложение № 1)

**ПАРОЛЬНАЯ ПОЛИТИКА**

**администрации городского округа «Вуктыл»**

**1. Общие положения**

Пароли являются важным элементом информационной безопасности. Они обеспечивают защиту учетных записей пользователей. Неправильно выбранный пароль может стать причиной неавторизованного доступа к конфиденциальной информации или нарушением работоспособности информационных систем администрации городского округа «Вуктыл» (далее по тексту – Организация). Все пользователи, имеющие доступ к информационным системам Организации, несут ответственность за принятие соответствующих (описываемых ниже) мер по созданию и защите пароля.

# 2. Цель

Целью политики является введение стандартов по созданию стойких паролей, их защите и срокам действия.

# 3. Область действия

Политика распространяется на всех пользователей информационных систем Организации, которые имеют учетные записи или назначены ответственными за таковые, а также на сотрудников, хранящих конфиденциальную информацию Организации.

# 4. Политика

### 4.1 Рекомендации по созданию пароля

Пароли используются для многочисленных целей. Наиболее распространенные из них: авторизация на персональном компьютере, авторизация в информационной системе и так далее.

Поскольку пароли используются многократно (за редким исключением информационных систем с одноразовыми паролями) пользователи должны знать требования по созданию стойких паролей.

**Характеристики слабого пароля:**

1. содержит менее 5 символов;
2. слово из словаря;
3. является повтором предыдущего пароля;
4. повседневно используемое слово, например, имена или фамилии друзей, коллег, актеров или сказочных персонажей, клички животных;
5. является словом на одном из языков, диалектов, жаргонов, сленгов;
6. компьютерный термин, команда, наименование организаций, веб-сайтов, аппаратного или программного обеспечения;
7. вариации наименования Организации или отдела;
8. день рождения или другая персональная информация, например, почтовый адрес, номер телефона и тому подобное;
9. регулярные последовательности символов и цифр, например, 111222, abcde, qwerty и тому подобное;
10. что-либо из перечисленного выше в обратном написании;
11. что-либо из перечисленного выше с добавлением цифр в начале или конце.

**Характеристики стойкого пароля:**

1. не менее 6 символов длиной;
2. не подходит под характеристики слабого пароля (см. определение выше);
3. состоит из комбинации не менее 3 групп символов:

1 группа - символы верхнего регистра;

2 группа - символы нижнего регистра;

3 группа - цифры;

4 группа - специальные символы;

5 группа - символы с большим ASCII кодом (вводятся удержанием кнопки ALT и набором ASCII-кода на цифровой клавиатуре);

1. не хранится и не передается в открытом виде.

Пароль должен хорошо запоминаться. Один из способов – создание пароля на основе названия песни или запоминающейся фразы. Например: «Это элементарно, Ватсон!», – «2Элмнт\_В!».

### 4.2 Защита паролей

Для учетных записей пользователей Организации запрещено использовать тот же самый пароль, что и для других информационных систем (например, домашний интернет-провайдер, бесплатная электронная почта, форумы и тому подобное). По возможности не используйте один и тот же пароль для различных систем Организации. Также желательно использовать различные пароли в операционных системах Unix и Windows.

Запрещено сообщать пароль кому бы то ни было, включая административный персонал и секретарей. Все пароли являются конфиденциальной информацией Организации.

**Список запрещенных действий с личными паролями:**

1. никому не сообщайте пароль по телефону;
2. не указывайте пароль в сообщениях электронной почты;
3. не сообщайте принципы создания пароля (например, «на основе знаменитой фразы Холмса»);
4. не сообщайте пароль в электронных опросах и незнакомых формах авторизации;
5. не сообщайте пароль членам семьи и родственникам;
6. не сообщайте пароль вашему руководству и коллегам;
7. не записывайте свой пароль на бумагу, не наклеивайте стикеры с записанными паролями на монитор компьютера;
8. не сохраняйте пароли в файлах на каком-либо носителе (например, флэшка, мобильный телефон и тому подобное) без шифрования.

Покидая рабочее место пользователь обязан заблокировать компьютер, нажав сочетание клавиш Win+L на клавиатуре (в ОС Windows).

Если кто-либо требует сообщить ваш пароль, сошлитесь на данный документ или направьте его к начальнику вашего структурного подразделения (о фактах требования пароля незамедлительно сообщайте начальнику вашего структурного подразделения).

Администратор информационной системы создаёт новую учётную запись со стандартным паролем. Этот пароль может передаваться пользователю по телефону, лично (исключая возможность перехвата сторонними лицами) или посредством корпоративной почты (желательно, чтобы в настройках почтовой программы было включено шифрование). При первом входе пользователь, которому предназначалась данная учётная запись, обязан сменить пароль.

При уходе в отпуск сотрудник Организации или ответственное лицо, делегирующие свои полномочия другому лицу, обязаны создать новую учётную запись для получения доступа к информационным ресурсам Организации и передать учётные данные замещающему сотруднику указанным в предыдущем абзаце способом.

Пароль должен изменяться не менее одного раза в 3 месяца. Рекомендованный интервал смены пароля 30 дней. Если вы подозреваете, что ваш пароль стал известен кому-либо, немедленно измените его и сообщите об этом начальнику своего структурного подразделения.

# 5. Ответственность

Все сотрудники Организации несут ответственность за нарушение данной политики в соответствии с законодательством Российской Федерации.

# 6. Контроль

Контроль за соблюдением настоящей политики возлагается на начальников структурных подразделений.

УТВЕРЖДЕНА

постановлением администрации

городского округа «Вуктыл»

от « \_\_\_» \_\_\_\_\_\_\_\_2017 г. № \_\_\_\_\_

(приложение № 2)

**ИНСТРУКЦИЯ**

**по антивирусной защите информации на автоматизированных**

**рабочих местах администрации городского округа «Вуктыл»**

1. Настоящая Инструкция определяет требования к организации антивирусной защиты информации на автоматизированных рабочих местах администрации городского округа «Вуктыл» (далее – АРМ) которые в обязательном порядке должны выполняться при организации и поддержке функционирования системы антивирусной защиты АРМ под управлением операционных систем Windows.
2. На АРМ применяются только лицензионные средства антивирусной защиты.
3. Антивирус на АРМ должен быть включен, а также должны быть работоспособны его модули, отвечающие за автоматическую проверку открываемых пользователями файлов и веб-ресурсов.
4. Антивирусные базы на АРМ должны быть не старше 4 рабочих дней (рекомендуемый срок), в крайнем случае — 2 недель.
5. Антивирусные базы на АРМ должны обновляться не реже 1 раза в день, рекомендуется — не реже 2 раз в день.
6. Доступ к настройкам антивируса на АРМ должен быть защищен паролем (при наличии данной функции).
7. Пользователи АРМ должны уведомляться средствами антивируса о критическом статусе на их АРМ, а также об обнаружении вредоносного программного обеспечения.
8. В случае наличия системы централизованного управления антивирусной защитой (далее – СЦАЗ), зарегистрированные компонентами антивирусной защиты события безопасности должны передаваться в СЦАЗ. Агент администрирования, подключенный к СЦАЗ, должен быть установлен на все АРМ. СЦАЗ должен осуществлять контроль за АРМ, на которых установлен агент администрирования.
9. Запрещается блокировать нормальную работу агента администрирования и антивируса.
10. При точной идентификации вируса модулем автоматической проверки открываемых пользователями файлов и веб-ресурсов, он должен автоматически удаляться или блокироваться.
11. Должна быть настроена ежедневная ночная антивирусная проверка всех файлов на дисках, не выключенных АРМ. При нахождении в ходе проверки вредоносного ПО, должна происходить только регистрация события безопасности, без удаления зараженного файла.
12. Должен осуществляться мониторинг и реагирование на события безопасности, регистрируемые антивирусом.
13. Развертывание компонентов, настройка, администрирование, обновление баз, а также контроль требований настоящей политики должны осуществляться максимально централизованно.
14. При обнаружении антивирусом в ходе проверки вредоносного программного обеспечения необходимо провести служебное разбирательство по выявленному инциденту информационной безопасности.
15. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на каждого пользователя АРМ. Пользователи, нарушившие требования настоящей Инструкции, привлекаются к дисциплинарной ответственности в соответствии с Трудовым кодексом Российской Федерации, а также в соответствии с действующим законодательством Российской Федерации.

УТВЕРЖДЕН

постановлением администрации

городского округа «Вуктыл»

от « \_\_\_» \_\_\_\_\_\_\_\_2017 г. № \_\_\_\_\_

(приложение № 3)

**ПЕРЕЧЕНЬ**

**базового (разрешенного) программного обеспечения для выполнения должностных обязанностей пользователей на автоматизированных рабочих местах администрации городского округа «Вуктыл»**

|  |  |  |
| --- | --- | --- |
| **Наименование программного обеспечения** | **Производитель** | **Категория программного обеспечения** |
| 7-Zip | Igor Pavlov | Архиватор |
| Adobe Flash | Adobe Systems Incorporated | Программное обеспечение для работы с flash |
| Adobe Reader | Adobe Systems Incorporated | Офисное программное обеспечение |
| Google Chrome  Яндекс браузер  Mozilla Firefox  Internet Explorer  Браузер Opera |  | ***Веб-браузеры –*** прикладное программное обеспечение для просмотра веб-страниц; содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями; а также для решения других задач |
| Java | Oracle | Дополнительные компоненты ОС |
| Pandion | Dries Staelens | ***Мессенджер –*** коммуникационная программа-клиент, позволяющая пользователям общаться друг с другом в реальном времени, используя различные виды коммуникаций: мгновенные сообщения, видео- и голосовую связь, общий доступ к рабочему столу, конференции, передачу файлов |
| Microsoft Office (с коробочной, электронной или корпоративной лицензией) | Microsoft Corporation | Программное обеспечение, предназначенное для работы с различными типами документов: текстами, электронными таблицами, базами данных и другое |
| Касперский | «Лаборатория Касперского» | Антивирусное ПО |
| Стандартное ПО Windows | Microsoft Corporation |  |
| Операционная система (Лицензионная копия Windows версии не ниже 7) | Microsoft Corporation | Комплекс взаимосвязанных программ, предназначенных для управления ресурсами вычислительного устройства и организации взаимодействия с пользователем |

* Использование иного лицензионного программного обеспечения, необходимого для выполнения должностных обязанностей пользователей ресурсов корпоративной информационно – телекоммуникационной сети администрации городского округа «Вуктыл», возможно, только после письменного запроса на установку и использование программного обеспечения в отдел информационных технологий администрации городского округа «Вуктыл».

УТВЕРЖДЕН

постановлением администрации

городского округа «Вуктыл»

от « \_\_\_» \_\_\_\_\_\_\_\_2017 г. № \_\_\_\_\_

(приложение № 4)

**РЕГЛАМЕНТ**

**работы пользователей автоматизированных рабочих мест администрации**

**городского округа «Вуктыл», подключенных к корпоративной сети передачи данных и информационно-телекоммуникационной сети «Интернет»**

**1. Общие положения**

* 1. Настоящий регламент работы пользователей автоматизированных рабочих мест, подключенных к корпоративной сети передачи данных и информационно-телекоммуникационной сети «Интернет» (далее – Регламент), устанавливает правила, регулирующие использование информационных ресурсов сети «Интернет» и определяет права, обязанности, запреты и ответственность пользователей автоматизированных рабочих мест, подключенных к корпоративной сети передачи данных и информационно-телекоммуникационной сети «Интернет» (далее – пользователь).
  2. Настоящий Регламент разработан в целях обеспечения информационной безопасности и персональной ответственности работниковадминистрации городского округа «Вуктыл» за использование информационных ресурсов сети «Интернет» в неслужебных целях.
  3. Требования настоящего Регламента распространяются на всех работников администрации городского округа «Вуктыл».
  4. В настоящем Регламенте используются следующие основные понятия:

1. пользователь – работник, осуществляющий текущую деятельность, связанную с выполнением трудовой функции посредством автоматизированного рабочего места, подключенного к корпоративной сети передачи данных и информационно-телекоммуникационной сети «Интернет»;
2. автоматизированное рабочее место – рабочее место пользователя, включая компьютер, оборудование, технические средства необходимые для осуществления текущей деятельности, связанной с выполнением трудовой функции пользователя как работника;
   1. Пользователь должен быть ознакомлен с настоящим Регламентом под роспись.

**2. Права пользователя**

Пользователь имеет право на:

1. получение доступа к имеющимся ресурсам корпоративной сети передачи данных, в том числе информационно-телекоммуникационной сети «Интернет» в пределах, установленных должностными обязанностями;
2. обращение в отдел информационных технологий администрации городского округа «Вуктыл» за справочной информационной и технической поддержкой.

**3. Обязанности пользователя**

Пользователь обязан:

1. соблюдать условия Регламента, иные требования, установленные локальными нормативными актами работодателя;
2. принимать меры по соблюдению требований законодательства Российской Федерации, законодательства Республики Коми при осуществлении текущей деятельности, связанной с выполнением трудовой функции посредством автоматизированного рабочего места;
3. производить антивирусный контроль автоматизированного рабочего места согласно инструкции по антивирусной защите информации;
4. не допускать заражения автоматизированного рабочего места вредоносным программным обеспечением (вирус);
5. незамедлительно уведомлять отдел информационных технологий администрации городского округа «Вуктыл»в случае обнаружения вредоносного программного обеспечения (вирус);
6. использовать программное обеспечение исключительно для выполнения трудовых функций;
7. информировать руководителя структурного подразделения о любых нарушениях, которые могут привести к несанкционированному доступу обрабатываемой информации или сбоям в работе сети.

**4. Запреты**

Пользователю запрещается:

1. вскрывать системный блок компьютера;
2. самостоятельно изменять настройки компьютера без разрешения отдела информационных технологий администрации городского округа «Вуктыл»;
3. самостоятельно устанавливать программное обеспечение (включая приложения).
4. использовать различные внешние носители информации, не проверенные на наличие компьютерных вирусов;
5. использовать ресурсы информационно - телекоммуникационной сети «Интернет» в неслужебных целях;
6. допускать к автоматизированному рабочему месту посторонних лиц;
7. работать на автоматизированном рабочем месте, осуществляя доступ к информационно - телекоммуникационной сети «Интернет» под чужой учетной записью;
8. передавать через информационно - телекоммуникационную сеть «Интернет» третьей стороне служебную и конфиденциальную информацию и свои учетные данные;
9. использовать информационно - телекоммуникационную сеть «Интернет» для приема, передачи и записи файлов мультимедиа (видео, музыка, игры, и так далее), не связанных с должностными обязанностями;
10. посещать социальные сети, а также сайты, не связанные с исполнением должностных обязанностей.

**5. Ответственность пользователя**

Пользователь несет ответственность за поддержание установленного в настоящем Регламенте порядка на автоматизированном рабочем месте. Пользователи, нарушившие требования настоящего Регламента, привлекаются к дисциплинарной ответственности в соответствии с Трудовым кодексом Российской Федерации, а также в соответствии с действующим законодательством Российской Федерации.