

**«КНЯЖПОГОСТ»**

**МУНИЦИПАЛЬНŐЙ РАЙОНСА**

**АДМИНИСТРАЦИЯ**

**АДМИНИСТРАЦИЯ**

# МУНИЦИПАЛЬНОГО РАЙОНА

**«КНЯЖПОГОСТСКИЙ»**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | ПОСТАНОВЛЕНИЕ |  |

от 12 ноября 2015г. № 664

|  |  |
| --- | --- |
| Об организации информационной безопасности на автоматизированных рабочих местах в администрации муниципального района «Княжпогостский» |  |

В соответствии с пунктом 1.6 раздела I протокола Межведомственной рабочей группы по информационной безопасности электронного правительства Республики Коми от 29 октября 2015 года № 2 Министерства массовых коммуникаций, информации и связи Республики Коми

ПОСТАНОВЛЯЮ:

1. Утвердить Парольную политику администрации муниципального района «Княжпогостский» согласно приложению № 1 к настоящему постановлению.

2. Утвердить Инструкцию по антивирусной защите согласно приложению № 2 к настоящему постановлению.

3. Утвердить Перечень разрешенного к использованию программного обеспечения согласно приложению №3 к настоящему постановлению.

4. Утвердить Регламент работы сотрудников администрации муниципального района «Княжпогостский», подключенных к корпоративной сети передачи данных и информационно-телекоммуникационной сети «Интернет» согласно приложению № 4 к настоящему постановлению.

5. Рекомендовать отраслевым (функциональным) подразделениям администрации муниципального района «Княжпогостский», руководителям администраций городских, главам сельских поселений муниципального района «Княжпогостский» принять аналогичные нормативно - правовые акты.

6. Управлению делами администрации муниципального района «Княжпогостский» ознакомить под роспись с вышеперечисленными документами сотрудников администрации.

7. Контроль за исполнением настоящего постановления возложить на начальника управления делами администрации муниципального района «Княжпогостский» Шепеленко Е.М.

|  |  |
| --- | --- |
| Руководитель администрации | В.И. Ивочкин |

Приложение № 1

к постановлению администрации

муниципального района «Княжпогостский»

от 12 ноября 2015 г. № 664

**Парольная политика**

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 нарушения работоспособности информационных систем администрации муниципального района «Княжпогостский» (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

### I. Положения для всех сотрудников Организации

### 4.1 Рекомендации по созданию пароля

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

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

***Характеристики слабого пароля*:**

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

***Характеристики стойкого пароля*:**

* не менее 6 символов длиной;
* не подходит под характеристики слабого пароля (см. определение выше);
* состоит из комбинации не менее 3-х 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);
* 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 т.п.). 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*:**

* никому не сообщайте пароль по телефону;
* не указывайте пароль в сообщениях электронной почты;
* не сообщайте принципы создания пароля (например, "на основе знаменитой фразы Холмса");
* не сообщайте пароль в электронных опросах и незнакомых формах авторизации;
* не сообщайте пароль членам семьи и родственникам;
* не сообщайте пароль вашему руководству и коллегам;
* не записывайте свой пароль на бумагу, не наклеивайте стикеры с записанными паролями на монитор компьютера;
* не сохраняйте пароли в файлах на каком-либо носителе (например, флэшка, мобильный телефон и т.п.) 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 отделов и заведующих секторами.

Приложение № 2

к постановлению администрации

муниципального района «Княжпогостский»

от 12 ноября 2015 г. № 664

**Инструкция по антивирусной защите**

1. Настоящая Инструкция определяет требования к организации антивирусной защиты информации на автоматизированном рабочем месте (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 четырех рабочих дней (рекомендуемый срок), в крайнем случае — двух недель.
5. Антивирусные базы на АРМ должны обновляться не реже одного раза в день, рекомендуется — не реже двух 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 ПО.
8. Запрещается блокировать нормальную работу антивируса.
9. При точной идентификации вируса модулем автоматической проверки открываемых пользователями файлов и веб-ресурсов, он должен автоматически удаляться или блокироваться.
10. 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.
11. Должен осуществляться мониторинг и реагирование на события безопасности, регистрируемые антивирусом.
12. Развертывание компонентов, настройка, администрирование, обновление баз, а также контроль требований настоящей политики должны осуществляться максимально централизованно.
13. При обнаружении антивирусом в ходе проверки вредоносного программного обеспечения необходимо провести служебное разбирательство по выявленному инциденту информационной безопасности.
14. 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.

Приложение 3

УТВЕРЖДЕНО:

постановлением администрации

муниципального района «Княжпогостский»

от « 12 » ноября 2015 г. № 664

**Перечень базового (разрешенного) программного обеспечения**

|  |  |  |
| --- | --- | --- |
| **Наименование программного обеспечения** | **Производитель** | **Категория программного обеспечения** |
| 7-Zip  WinRAR | Igor Pavlov  Евгений Рошал, Александр Рошал | Архиватор |
| Adobe Flash | Adobe Systems Incorporated | Программное обеспечение для работы с flash |
| Adobe Reader  Foxit Reader | Adobe Systems Incorporated  Foxit Corporation | 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 |
| Microsoft Lync (Skype for Business) | Microsoft Corporation | ***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 др. |
| Касперский | «Лаборатория Касперского» | Антивирусное ПО |
| Стандартное ПО Windows | Microsoft Corporation |  |
| Операционная система MS Windows | 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 Республики Коми, возможно, только с ответственным за информационную безопасность на автоматизированных рабочих местах.

Приложение 4

УТВЕРЖДЕНО:

постановлением администрации

муниципального района «Княжпогостский»

от « 12 » ноября 2015 г. № 664

**РЕГЛАМЕНТ**

работы сотрудников администрации муниципального района

«Княжпогостский»,

подключенных к корпоративной сети передачи данных и информационно-телекоммуникационной сети «Интернет»

**I. Общие положения**

* 1. Настоящий Типовой 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 сотрудников администрации муниципального района «Княжпогостский» за использование информационных ресурсов сети «Интернет» в неслужебных целях.
  3. Требования настоящего Регламента распространяются на всех сотрудников администрации муниципального района «Княжпогостский».
  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.

**II. Права пользователя**

* 1. 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 к работодателю за справочной информационной и технической поддержкой;

**III. Обязанности пользователя**

3.1. 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;
4. не допускать заражения автоматизированного рабочего место вредоносным программным обеспечением (вирус);
5. незамедлительно уведомлять ответственного за информационную безопасность автоматизированных рабочих местработодателяв 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.

**IV. Запреты**

4.1. Пользователю запрещается:

1. вскрывать системный блок компьютера;
2. самостоятельно изменять настройки компьютера без разрешения работодателя или иного уполномоченного лица;
3. самостоятельно устанавливать программное обеспечение (включая приложения), которое не входит в перечень разрешенного к использованию программного обеспечения.
4. использовать различные внешние носители информации, не проверенные на наличие компьютерных вирусов;
5. использовать ресурсы информационной сети Интернет в неслужебных целях;
6. допускать к автоматизированному рабочему месту посторонних лиц;
7. работать на автоматизированном рабочем месте, осуществляя доступ к сети Интернет под чужой учетной записью;
8. передавать через сеть Интернет третьей стороне служебную и конфиденциальную информацию и свои учетные данные;
9. использовать сеть Интернет для приема, передачи и записи файлов мультимедиа (видео, музыка, игры, и т.д.), не связанных с должностными обязанностями;
10. посещать социальные сети, а также сайты, не связанные с исполнением должностных обязанностей.

**V. Ответственность пользователя**

5.1. 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.