**АДМИНИСТРАЦИЯ БРЕЖНЕВСКОГО СЕЛЬСОВЕТА**

**КУРСКОГО РАЙОНА КУРСКОЙ ОБЛАСТИ**

**ПОСТАНОВЛЕНИЕ**

**от 27.03.2020г. № 32-П**

|  |
| --- |
|  |

**Об утверждении Положения об учете, хранении и использовании носителей электронной подписи**

**в Администрации Брежневского сельсовета**

**Курского района Курской области**

В соответствии с постановлением Правительства Российской Федерации

от 1 ноября 2012г.№1119г ."Об утверждении требований к защите персональных

Данных при их обработке в информационных системах персональных данных» и приказом Федеральной службы по техническому и экспортному контролю от

18 февраля 2013г.№21"Об утверждении состава и содержания организационных и

технических мер по обеспечению безопасности персональных данных при их

обработке в информационных системах персональных данных»

Администрация Брежневского сельсовета Курского района Курской области

ПОСТАНОВЛЯЕТ:

1.Утвердить прилагаемое Положение об учете, хранении и использовании

Носителей электронной подписи в Администрации Брежневского сельсовета Курского района Курской области.

2.Заместителю Главы Администрации Брежневского сельсовета Курского района по общим вопросам довести настоящее постановление до сведения

Сотрудников администрации.

3. Контроль за выполнением настоящего постановления оставляю за собой.

4. Настоящее постановление вступает в силу со дня подписания.

Глава Брежневского сельсовета

Курского района Курской области В.Д.Печурин

|  |  |
| --- | --- |
|  | Приложениек постановлению АдминистрацииБрежневского сельсовета Курского района Курской областиот 27.03.2020г. № 32-П |

**ПОЛОЖЕНИЕ**

**Об учете, хранении и использовании носителей электронной подписи в**

**Администрации Брежневского сельсовета Курского района Курской области**

**I. Общие положения**

1.Положение об учете, хранении и использовании носителей электронной подписи в Администрации Брежневского сельсовета Курского района Курской области (далее соответственно - Положение, Администрация) устанавливает организационные мероприятия по работе с носителями электронных подписей (далее - НЭП), порядок изготовления, регистрации, предоставления доступа, учета, хранения и использования работниками НЭП, контроля использования НЭП, порядок действий при компрометации НЭП, а также правила обеспечения режима безопасности при работе с НЭП.

2.Положение разработано в соответствии с нормативными правовыми актами

Российской Федерации в области защиты информации, том числе Федеральным

Законом от 06 апреля 2013 года № 63-ФЗ «Об электронной подписи».

3.Требования, установленные настоящим Положением, являются обязательными для всех работников администрации.

4.Работник, прежде чем приступить к работе с НЭП, обязан ознакомиться с

настоящим положением лично, под роспись.

**II Основные термины, сокращения и определения**

5.Носитель электронной подписи - дискета, флэш-память, рутокен и или прочие электронные носители, на которых хранятся ключи

Электронной подписи, предназначенные для защиты электронных взаимодействий.

6.Секретный (закрытый) ключ подписи ключ, предназначенный для

формирования электронной подписи электронных документов.

7.Открытый (публичный) ключ подписи ключ, автоматически формируется при изготовлении секретного ключа подписи и однозначно зависящий от него. Открытый ключ предназначен для проверки корректности электронной подписи электронного документа. Открытый ключ считается принадлежащим участнику электронных

взаимодействий, если он был сертифицирован (зарегистрирован) в установленном порядке.

8.Ключ шифрования ключ, предназначенный для закрытия электронного

документа при электронных взаимодействиях.

9.Шифрование специализированный метод защиты информации от

Ознакомления с ней третьих лиц, основанный на кодировании информации по

Алгоритму ОСТ 28147-89 с использованием соответствующих ключей.

11. Компрометация- утрата, хищение, несанкционированное копирование или подозрение на копирование НЭП или любые другие ситуации, при которых достоверно неизвестно, что произошло с НЭП. К компрометации также относится увольнение работников, имевших доступ к электронной подписи. Сертификация ключа – процедура заверения (подписания) открытой части регистрируемого ключа электронной подписью.

12.Заявка на регистрацию ключа – служебное сообщение, содержащее новый открытый ключ, подписанное электронной подписью.

13. Информационная безопасность (далее - ИБ) – комплекс правовых, организационных и технических мер, обеспечивающих конфиденциальность, целостность и доступность информации.

14. Информационная инфраструктура (далее - ИИ) – информационные ресурсы, технологии и системы, базы данных, серверное, компьютерное, сетевое и периферийное оборудование, программное обеспечение, программные и аппаратно-программные средства защиты информации, информационно-телекоммуникационная сеть, находящиеся в ведении администрации, используемые для выполнения работниками администрации служебных обязанностей, доступа к ресурсам сети Интернет, а также информационного взаимодействия с органами государственной власти Курской области.

15. Информационные технологии (далее - ИТ) – совокупность методов и процессов информации администрации с использованием средств компьютерной техники и телекоммуникационного оборудования.

16. Сеть Интернет – глобальная информационно-телекоммуникационная сеть, обеспечивающая удаленный доступ к ресурсам различного содержания и направленности.

17. Пользователь – работник администрации, использующий ресурсы информационной инфраструктуры администрации при исполнении своих служебных обязанностей.

18. Автоматизированное рабочее место (далее - АРМ) – в составе персонального компьютера, периферийного оборудования и прикладного программного обеспечения, предназначенное для исполнения пользователем служебных обязанностей.

19. Паспорт АРМ -документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

**III. Организация работы с носителями ключевой информации**

20 .Пользователь НЭП, которому в соответствии с его должностными функциями предоставлено право постановки на электронных документах электронной подписи, несет персональную ответственность за сохранность и правильное использование вверенной ему ключевой информации и содержание документов, на которых стоит его электронная подпись. Список лиц, имеющих доступ к НЭП, составляется ответственным по информационной безопасности и фиксируется в постановлении администрации.

21. В целях обеспечения идентификации отправителей и получателей информации, защиты ее от несанкционированного доступа глава администрации назначает ответственных работников за осуществление электронного взаимодействия и наделяет их правом установки электронной подписи отправляемых документов.

22. Ответственный по информационной безопасности устанавливает соответствующие средства криптозащиты информации на АРМ работников администрации для обеспечения электронного взаимодействия .Проводит обучение ответственных работников администрации, участвующих в электронных взаимодействиях, работе со средствами обеспечения электронного документооборота и средствами криптозащиты информации.

23. Ответственный по информационной безопасности осуществляет выборочный контроль соблюдения ответственными работниками комитета правил обеспечения режима безопасности НЭП.

**IV. Порядок изготовления, регистрации, предоставления доступа, учета,**

**хранения и использования носителей электронных подписей**

25.Генерация и запись на НЭП уникальной ключевой информации, необходимой для формирования электронной подписи, осуществляется ответственным по информационной безопасности с помощью программного обеспечения, выполняющего функции, регламентированные технологическим процессом формирования ключей электронной подписи.

26. Работник Администрации, для которого изготавливалась электронная подпись, оформляет необходимую документацию для изготовления электронной подписи.

27. Электронная подпись изготавливается и записывается на НЭП в аккредитованных Министерством связи и массовых коммуникаций Российской Федерации удостоверяющих центрах.

28. Работник Администрации, для которого изготавливалась электронная подпись, по доверенности получает электронную подпись в аккредитованном удостоверяющем центре.

29. Для обеспечения возможности восстановления электронной подписи работника Администрации, в случае выхода НЭП из строя, ответственный по информационной безопасности создает резервную копию электронной подписи.

30. Носители электронной подписи должны иметь соответствующие опознавательные ярлыки с регистрационными номерами.

31. НЭП ответственного работника Администрации может быть использована другим работником Администрации.

32. За хранение рабочей копии НЭП отвечает работник Администрации, для которого изготавливалась электронная подпись. Рабочие копии НЭП хранятся индивидуально.

33. Пользователю НЭП запрещается:

1. оставлять НЭП без личного присмотра;
2. делать неучтенные копии электронной подписи;
3. использовать НЭП в качестве носителя электронных документов и файлов, не имеющих отношения к техническому процессу подписания электронных документов электрон
4. изменения в файлы, находящиеся на НЭП;
5. использовать НЭП на заведомо неисправном АРМ;
6. подписывать своей электронной подписью любые электронные сообщения и документы, кроме тех видов документов, которые регламентированы технологическим процессом;
7. распространять информацию, что он является пользователем НЭП.

**V. Порядок действий при компрометации НЭП**

34. К событиям, связанным с компрометацией ключевой информации, должны быть отнесены следующие события:

1. утрата НЭП; утрата НЭП с последующим обнаружением;
2. увольнение работников администрации, имевших доступ к НЭП;
3. возникновение подозрений на
4. утечку информации или ее искажения в системе связи;
5. не расшифровывание входящих или исходящих сообщений;

35. При компрометации электронной подписи участника электронного взаимодействия предусмотрены следующие мероприятия:

1. Прекращение передачи информации с использованием скомпрометированной электронной подписи;
2. Сообщение о факте компрометации ответственному по информационной безопасности;
3. на основании сообщения участника электронного взаимодействия ответственный по информационной безопасности исключает из средств криптографической защиты информации скомпрометированную электронную подпись;
4. участник обмена электронного взаимодействия подготавливает документы на отзыв скомпрометированной электронной подписи из аккредитованного удостоверяющего центра.

**VI. Обеспечение информационной безопасности при работе с НЭП**

36. Порядок допуска в помещения, в которых ведется обработка НЭП, определяется внутренней инструкцией.

37. Для хранения носителей электронных подписей, нормативной и эксплуатационной документации, инсталляционных файлов помещения должны быть обеспечены сейфами.

38. Установленный порядок охраны помещений предусматривает периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

39. Размещение и установка средств криптографической защиты информации осуществляется в соответствии с требованиями документации на средства криптографической защиты.

40. Системные блоки АРМ со средствами криптографической защиты оборудованы средствами контроля их вскрытия.

41. Порядок обеспечения безопасности хранения НЭП:

1. Хранение электронных подписей, инсталляционных файлов и лицензий средств криптографической защиты информации допускается в одном хранилище с другими документами при условиях, исключающих и непреднамеренное уничтожение, или иное, непредусмотренное правилами пользования средствами криптозащиты информации, применение;
2. Действующие электронные подписи, записанные на носитель, должны храниться в сейфе ответственного лица за электронное взаимодействие. Возможность копирования и несанкционированного использования электронной подписи посторонним лицом должна быть исключена;

42. К работе со средствами криптографической защиты и носителям ключевой информации допускаются только работники администрации, знающие правила их эксплуатации, владеющие практическими навыками работы на АРМ, изучившие правила пользования и эксплуатационную документацию по средствам криптографической защиты, имеющие представления о возможных угрозах информации при ее обработке, передаче, хранении, методах и средствах защиты информации.

43. Уничтожение ключевой информации на НЭП должно производиться путем полного переформатирования носителя в количестве 7 раз.

44. Уничтожение НЭП, пришедшего в негодность, должно производиться путем расплавления на огне (сожжения) или измельчения микросхемы извлеченной из корпуса.