АДМИНИСТРАЦИЯ АЛТАЙСКОГО РАЙОНА
АЛТАЙСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ

23.04. 2018 г. № 581

с. Алтайское

О мерах по защите персональных данных в Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях

В соответствии с Федеральными законами от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 27.07.2006 N 152-ФЗ "О персональных данных", постановлением Правительства РФ 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", постановляю:

1. Назначить лицом, ответственным за организацию защиты информации конфиденциального характера и обработку персональных данных в Администрации Алтайского района Алтайского края, заведующего отделом программного обеспечения Администрации района Е.А.Соколовского.

2. Утвердить прилагаемые:

- Положение об обеспечении безопасности информации конфиденциального характера, обрабатываемой в Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях;
- Положение об обеспечении безопасности персональных данных при их обработке в Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях;
- Инструкцию по работе пользователей в информационных системах Администрации Алтайского района, структурных подразделениях и подведомственных организациях;
- Инструкцию по организации обслуживания и ремонта технических средств в информационных системах Администрации Алтайского района, ее структурных подразделениях и подведомственных организациях;
- Инструкцию по организации парольной защиты в информационных системах Администрации Алтайского района Алтайского края, структурных подразделениях и подведомственных организациях;
- Инструкцию по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа;

- Инструкцию по организации резервного копирования информации в информационных системах Администрации Алтайского района, ее структурных подразделениях и подведомственных организациях;

- Инструкцию по проведению антивирусного контроля в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях;

- Инструкцию по обращению с носителями ключевой информации в информационных системах персональных данных Администрации Алтайского района Алтайского края;

- Порядок доступа муниципальных служащих и иных работников Администрации Алтайского района Алтайского края в помещения, в которых ведется обработка персональных данных;

- Правила осуществления в Администрации Алтайского района и ее структурных подразделениях внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

- Перечень персональных данных, обрабатываемых в Администрации Алтайского района Алтайского края, в связи с реализацией служебных (трудовых) отношений;

- Типовое обязательство работника Администрации Алтайского района Алтайского края, непосредственно осуществляющего обработку персональных данных, о неразглашении персональных данных;

- Типовую форму согласия на обработку персональных данных муниципальных служащих Администрации Алтайского района Алтайского края;

- Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

- Типовую форму журнала учета и выдачи машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа.

3. Контроль за исполнением настоящего постановления возложить на заместителя главы Администрации района К.Ю.Косых.

Глава Алтайского района С.В.Черепанов

УТВЕРЖДЕНО
постановлением Администрации
Алтайского района
от 23.04.2018 года № 581

ПОЛОЖЕНИЕ
об обеспечении безопасности информации конфиденциального характера, обрабатываемой в Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях

1. Общие положения

1.1. Типовое положение об обеспечении безопасности информации конфиденциального характера, обрабатываемой в Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях (далее – «Положение»), разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», со Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2002 № 282, а также на основании других нормативных правовых актов, методических документов Российской Федерации, регулирующих отношения, связанные с обработкой и защитой информации конфиденциального характера.

1.2. Под информацией конфиденциального характера понимается информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Перечни сведений конфиденциального характера утверждаются главой района, председателями комитетов и директорами подведомственных организаций (далее – «организация»).

1.3. Настоящее Положение устанавливает требования к обеспечению безопасности информации конфиденциального характера, обрабатываемой в информационных системах организации.

Под информационной системой (далее – ИС) понимается совокупность информации, содержащейся в базах данных, и обеспечивающих ее обработку информационных технологий, технических средств организации.

1.4. Безопасность информации конфиденциального характера при ее обработке в ИС обеспечивается применением организационных и технических мер.

1.5. Требования настоящего Положения являются обязательными для исполнения всеми лицами, получившими доступ к информации конфиденциального характера, и должны быть доведены до их сведения.

1.6. Решение о необходимости внесения изменений в Положение принимается на основании:

изменения нормативных правовых актов и методических документов, регулирующих отношения, связанные с обработкой и защитой информации конфиденциального характера;

результатов анализа инцидентов информационной безопасности в организации;

изменения технологии хранения и обработки информации конфиденциального характера.

1.7. Все изменения Положения до их ввода в действие подлежат предварительной оценке на соответствие нормативным правовым актам и методическим документам, регулирующим отношения, связанные с обработкой и защитой информации.

2. Цель и требования защиты информации

2.1. Основной целью Положения является принятие организационных и технических мер, направленных:

на обеспечение защиты информации от несанкционированного доступа, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении такой информации;

на соблюдение конфиденциальности информации;

на реализацию права на доступ к конфиденциальной информации.

2.2. На основании Положения устанавливаются требования:

к разграничению доступа к информации конфиденциального характера, порядку и условиям такого доступа;

к порядку хранения и обработки информации конфиденциального характера;

к передаче информации конфиденциального характера другим лицам по договору или на ином установленном законом основании.

3. Методы и способы защиты информации конфиденциального характера, обрабатываемой в ИС

3.1. Для достижения цели защиты информации конфиденциального характера системы безопасности должны обеспечивать эффективное решение следующих задач:

предотвращение несанкционированного доступа к информации конфиденциального характера и (или) передачи ее лицам, не имеющим права на доступ к ней;

своевременное обнаружение фактов несанкционированного доступа;

предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации конфиденциального характера;

недопущение воздействия на технические средства обработки информации конфиденциального характера, в результате которого нарушается их функционирование;

создание возможности восстановления информации конфиденциального характера, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянный контроль за обеспечением защищенности информации конфиденциального характера.

3.2. Выполнение требований настоящего Положения регламентируется следующими документами:

инструкция по работе пользователей в ИС;

инструкция по организации парольной защиты в ИС;

инструкция по организации резервного копирования информации в ИС;

инструкция по проведению антивирусного контроля в ИС;

инструкция по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа;

инструкция по организации обслуживания и ремонта технических средств в ИС;

инструкция по организации доступа в помещения, в которых осуществляется обработка информации, в том числе персональных данных и иной информации конфиденциального характера;

типовая форма журнала учета и выдачи машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа.

3.3. Помещения, в которых ведется обработка информации конфиденциального характера, должны соответствовать режимным требованиям, должна обеспечиваться сохранность ИС, носителей информации конфиденциального характера и средств защиты информации, а также исключаться возможность неконтролируемого пребывания посторонних лиц в этих помещениях.

3.4. Обработка документов с пометкой «для служебного пользования» допускается только в ИС, аттестованных по требованиям безопасности информации.

4. Обязанности

4.1. Руководитель организации:

организует работу сотрудников организации в ИС;

утверждает расходы на финансовое, материально-техническое и иное обеспечение мероприятий по функционированию ИС.

4.2. Подразделение или лицо, ответственное за защиту информации в организации:

организует защиту информации конфиденциального характера, обрабатываемой в ИС;

определяет порядок доступа к информации конфиденциального характера, обрабатываемой в ИС;

осуществляет методическое руководство и внесение предложений по организации и совершенствованию систем защиты информации;

отвечает за соблюдение требований по обеспечению безопасности информации, обрабатываемой в ИС;

отвечает за обнаружение фактов несанкционированного доступа к ИС;

организует аттестацию по требованиям безопасности информации ИС, предназначенных для обработки документов с пометкой «для служебного пользования»;

осуществляет администрирование ИС, аттестованных по требованиям безопасности информации;

организует и обеспечивают работы по проведению антивирусного контроля ИС;

осуществляет резервное копирование и восстановление информации конфиденциального характера, обрабатываемой в ИС.

4.3. Подразделение или лицо, ответственное за администрирование ИС в организации:

сопровождает функционирование программного обеспечения ИС в присутствии представителей подразделения, ответственного за защиту информации в организации, либо лица, но которого возложены обязанности по обеспечению информационной безопасности в организации;

проводит обслуживание ИС, периферийного и другого специализированного оборудования в присутствии представителей подразделения, ответственного за защиту информации в организации, либо лица, но которого возложены обязанности по обеспечению информационной безопасности в организации.

4.4. Подразделение или лицо, ответственное за кадровый учет в организации, уведомляет сотрудников подразделения, ответственного за защиту информации в организации, либо лицо, но которого возложены обязанности по обеспечению информационной безопасности в организации об изменении кадрового состава.

4.5. Пользователи ИС:

отвечают за соблюдение установленного порядка использования ИС;

соблюдают требования нормативных документов по обеспечению безопасности информации конфиденциального характера, обрабатываемой в ИС;

соблюдают порядок доступа к ИС и информации конфиденциального характера, обрабатываемой ими;

осуществляют обработку документов с пометкой «для служебного пользования» в аттестованных по требованиям безопасности информации ИС;

не имеют права на изменение компонентов ИС, отключение или изменение настроек средств антивирусной защиты.

5. Ответственность

5.1. Ответственность за реализацию и соблюдение требований Положения возлагается на начальников структурных подразделений, пользователей ИС и лиц, ответственных за защиту информации в организации.

5.2. Нарушение требований Положения влечет ответственность в соответствии с действующим законодательством Российской Федерации.

6. Контроль состояния защиты информации конфиденциального характера

6.1. Контроль и надзор за выполнением требований по обеспечению безопасности информации конфиденциального характера при обработке в ИС осуществляется ФСТЭК России, ФСБ России в пределах их полномочий и без права ознакомления с информацией конфиденциального характера, обрабатываемой в ИС.

6.2. Повседневный контроль принятия организационных и технических мер, направленных на обеспечение защиты информации конфиденциального характера при обработке в ИС, осуществляется подразделением или лицом, ответственным за защиту информации в организации, в помещении режимно-секретного подразделения – его начальником.

УТВЕРЖДЕНО
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях

1. Общие положения

1.1. Типовое положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях (далее – «Положение») разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.
1.2. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях (далее – «организация», «оператор персональных данных»).
1.3. Безопасность персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) обеспечивается применением организационных мер и технических средств защиты информации (в том числе средств предотвращения несанкционированного доступа). Организационные меры и технические средства защиты информации должны удовлетворять требованиям, установленным нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИСПДн.
1.4. Требования настоящего Положения являются обязательными для исполнения всеми лицами, получившими доступ к персональным данным.
1.5. Решение о необходимости изменения этого Положения принимается на основании:
результатов проведенных аудитов, мероприятий по контролю и надзору за обеспечением безопасности персональных данных, осуществляемых уполномоченными органами;
изменения нормативных правовых актов и (или) нормативных методических документов Российской Федерации в области защиты персональных данных;
изменения процессов обработки персональных данных в ИСПДн оператора персональных данных;
результатов анализа инцидентов информационной безопасности в ИСПДн.
Изменения Положения должны быть направлены на предотвращение инцидентов или устранение последствий уже реализованных инцидентов информационной безопасности.
Все предлагаемые изменения Положения подлежат предварительной оценке до их ввода в действие на соответствие нормативным правовым актам и нормативным методическим документам Российской Федерации, регулирующим отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИСПДн.

2. Обработка персональных данных

2.1. Оператор персональных данных осуществляет обработку персональных данных лиц, замещающих должности муниципальной службы и должности, не относящиеся к должностям муниципальной службы, а также лиц, не являющихся сотрудниками оператора.
2.2. Обработка персональных данных осуществляется оператором персональных данных в целях реализации возложенных на него функций, определяемых законами и иными нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИСПДн.
2.3. Объем и характер обрабатываемых персональных данных должен соответствовать целям их обработки. Обрабатываемые персональные данные должны соответствовать заявленным целям обработки. Недопустимо объединение созданных для несовместимых между собой целей баз данных ИСПДн.
2.4. Обработка персональных данных осуществляется оператором персональных данных без проведения мероприятий по обезличиванию персональных данных.
2.5. Персональные данные оператор получает непосредственно от субъектов персональных данных, которые принимают решение об их предоставлении и дают согласие на их обработку своей волей и в своем интересе.
2.6. Лица, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списков сотрудников, допущенных к соответствующим персональным данным.
2.7. Принятые в организации организационно-распорядительные документы доводятся до сведения лиц, участвующих в процессе обработки персональных данных в части их касающейся.
2.8. Персональные данные, используемые для обработки в ИСПДн, порядок их использования, цель, периодичность и основания внесения изменений и дополнений в организационные документы, а также порядок хранения персональных данных устанавливаются оператором персональных данных.
2.9. Оператор персональных данных не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.
2.10. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, должно осуществляться не дольше, чем этого требуют цели обработки персональных данных. Персональные данные подлежат уничтожению по достижении всех целей их обработки или в случае утраты необходимости в достижении этих целей. Оператор персональных данных по согласованию с субъектом персональных данных может изменить сроки хранения его персональных данных в связи с обязанностями, возлагаемыми на оператора персональных данных законодательством Российской Федерации.

3. Обязанности и права оператора персональных данных в ИС

3.1. Оператор персональных данных обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или

не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.2. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.3. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.4. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.5. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

3.6. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

3.7. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 3.4 - 3.6 настоящего Положения, оператор осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

4. Методы и способы защиты персональных данных в ИСПДН

4.1. С целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных, оператором персональных данных должны быть установлены уровни защищенности персональных данных ИСПДн.

4.2. В целях обеспечения безопасности персональных данных определяются угрозы безопасности, оценивается актуальность угроз безопасности персональных данных. В результате разрабатывается модель угроз безопасности персональных данных.

Модель угроз безопасности персональных данных корректируется при изменении состава основных технических средств и условий эксплуатации ИСПДн сотрудниками подразделения или лицом, ответственным за защиту информации в организациях.

4.3. Установка, изменение (обновление) и удаление программного обеспечения в ИСПДн производится администратором безопасности информационных систем или в его присутствии.

4.4. Доступ лиц к ИСПДн, не допущенных к работе с персональными данными, должен быть исключен. ИСПДн должны быть защищены аппаратными и (или) программными средствами защиты информации от несанкционированного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИСПДн.

4.5. Обработка персональных данных в ИСПДн осуществляется с использованием средств защиты информации в соответствии с установленными требованиями нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обеспечением безопасности информации.

4.6. Охрана помещений, в которых ведется работа с персональными данными, и организация режима безопасности в этих помещениях должна обеспечивать сохранность технических средств и носителей персональных данных, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц. Все носители персональных данных должны быть учтены с помощью их маркировки, а их учетные данные занесены в журнал учета с отметкой об их выдаче (приеме).

4.7. В целях обеспечения безопасности персональных данных должны быть разработаны следующие организационно-распорядительные и организационно-методические документы по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн:

перечень ИСПДн организации;

перечень персональных данных, обрабатываемых в организации в связи с реализацией служебных (трудовых) отношений;

список лиц, допущенных к соответствующим персональным данным;

инструкция по работе пользователей в информационных системах организации;

инструкция по организации доступа в помещения, в которых ведется обработка персональных данных;

инструкция администратора безопасности информационных систем организации;

инструкция по организации резервного копирования информации в организации;

инструкция по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения персональных данных;

инструкция по организации парольной защиты в информационных системах организации;

инструкция по проведению антивирусного контроля в информационных системах организации;

инструкция по организации технического обслуживания и ремонта технических средств

информационных систем организации;
инструкция по правилам обращения с носителями ключевой информации в информационных системах организации;
инструкция ответственного за организацию обработки персональных данных организации;
правила рассмотрения запросов субъектов персональных данных или их представителей в организации;
правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в организации;
правила обработки персональных данных в организации;
другие организационно-распорядительные документы по обеспечению безопасности персональных данных, обрабатываемых в информационных системах организации.
4.8. Лица, уполномоченные осуществлять обработку персональных данных, несут ответственность за соблюдение требований по защите персональных данных в порядке, предусмотренном действующим законодательством Российской Федерации.

5. Обязанности и права должностных лиц

5.1. Руководитель организации:

организует разработку, внедрение, совершенствование и эксплуатацию системы защиты ИСПДн, а также организует внутренний контроль за соблюдением нормативных правовых актов Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

осуществляет финансовое, материально-техническое и иное обеспечение мероприятий по защите персональных данных при их обработке в ИСПДн организации по вопросам государственной службы и кадров;

назначает ответственного за организацию обработки персональных данных;
назначает ответственного за обеспечение безопасности персональных данных;
назначает администратора безопасности информационных систем.
5.2. Ответственный за организацию обработки персональных данных:
осуществляет внутренний контроль за соблюдением оператором персональных данных и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
доводит до сведения работников оператора персональных данных положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
организует и осуществляет прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.
5.3. Ответственный за обеспечение безопасности персональных данных:
несет ответственность за организацию обеспечения безопасности персональных данных при их обработке в информационных системах организации;

организует выполнение мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИСПДн;

организует расследование причин и условий появления нарушений безопасности ИСПДн, разработку предложений по устранению недостатков и предупреждению подобного рода нарушений;
разрабатывает проекты распорядительных документов по защите персональных данных при их обработке в ИСПДн в организации;
разрабатывает совместно с другими структурными подразделениями организации настоящее Положение и вносит в него в установленном порядке изменения;
разрабатывает предложения по дальнейшему совершенствованию системы защиты персональных данных при их обработке в ИСПДн;
осуществляет планирование мероприятий по защите персональных данных при их обработке в ИСПДн, их выполнение и контроль их эффективности;

подготавливает предложения о привлечении к проведению работ по защите персональных данных при их обработке в ИСПДн на договорной основе организаций, имеющих лицензию на соответствующий вид деятельности.

5.4. Администратор безопасности информационных систем:

обеспечивает обнаружение фактов несанкционированного доступа к ИСПДн, о которых должен доложить ответственному за обеспечение безопасности персональных данных;

осуществляет установку и ввод в эксплуатацию средств защиты информации ИСПДн в соответствии с эксплуатационной и технической документацией;

обеспечивает работы по проведению антивирусного контроля в ИСПДн;

выполняет резервное копирование персональных данных;

осуществляет установку (обновление версий) программного обеспечения ИСПДн, обеспечивает его функционирование;

осуществляет установку, подключение и настройку технических средств ИСПДн в соответствии с технической документацией;

осуществляет установку (развертывание) новых ИСПДн или подключение дополнительных устройств (узлов, блоков), необходимых для решения конкретных задач;

организует регистрацию и осуществляет учет защищаемых носителей информации.

5.5. Подразделение или лицо, ответственное за техническое обслуживание средств вычислительной техники в организации обеспечивает обслуживание и ремонт сетевого оборудования, рабочих станций, серверного и периферийного оборудования в ИСПДн.

6. Контроль состояния защиты персональных данных

6.1. Контроль и надзор за выполнением требований по обеспечению безопасности персональных данных при их обработке в ИСПДн, установленных Правительством Российской Федерации, осуществляется федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, а также уполномоченным органом по защите прав субъектов персональных данных в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в ИСПДн.

6.2. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИСПДн, осуществляется ответственным за организацию обработки персональных данных и ответственным за обеспечение безопасности персональных данных.

7. Заключительные положения

7.1. Настоящее Положение вступает в силу с момента его утверждения.

7.2. Настоящее Положение не заменяет собой действующее законодательство Российской Федерации, регулирующее отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИСПДн.

УТВЕРЖДЕНА
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ИНСТРУКЦИЯ
по работе пользователей в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях

1. Общие положения

1.1. Данная инструкция определяет общие принципы работы пользователей в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях (далее - ИС). Пользователи ИС несут персональную ответственность за свои действия.

1.2. Допуск пользователей для работы в ИС осуществляется в соответствии с их должностными обязанностями после ознакомления с документами по работе в ИС.

1.3. Доступ пользователей в ИС обеспечивает администратор безопасности ИС.

2. Порядок работы пользователей в ИС

2.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ИС, присвоенными администратором безопасности ИС. При этом для хранения информации ограниченного доступа разрешается использовать только учтенные носители информации (дискеты, компакт-диски, USB Flash-накопители, жесткие диски и т.д.), учтенные по журналу учета и выдачи машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа.

2.2. Пользователь ИС отвечает за правильность включения и выключения ПЭВМ, входа/выхода в/из ИС и действия при работе в ней.

2.3. Вход пользователя в ИС осуществляется на основе ввода (по запросу системы) имени (идентификатора), присвоенного при регистрации администратором безопасности ИС, и пароля. Требования к сложности пароля и периодичности его замены установлены в типовой инструкции по организации парольной защиты в ИС.

2.4. В случае отказа ИС в идентификации пользователя, либо не подтверждения личного пароля следует немедленно обратиться к администратору безопасности ИС.

2.5. Резервное копирование, уничтожение и восстановление защищаемой информации осуществляются пользователем в рамках выделенных полномочий, либо администратором безопасности ИС, в соответствии с инструкцией по организации резервного копирования информации в ИС.

2.6. Перед началом работы с носителями информации пользователь ИС обязан проверить их на наличие вредоносного программного обеспечения с использованием антивирусного программного обеспечения, установленного в ИС, в соответствии с инструкцией по проведению антивирусного контроля в ИС. В случае обнаружения вредоносного программного обеспечения на носителе информации пользователь обязан немедленно сообщить администратору безопасности ИС.

3. В процессе работы пользователю запрещается:

3.1. использовать для хранения и обработки защищаемой информации носители, не учтенные соответствующим образом;

3.2. осуществлять попытки неправомерного доступа к ресурсам ИС других пользователей;

3.3. пытаться подменять функции администратора безопасности ИС по перераспределению времени работы и полномочий доступа к ресурсам ИС;

3.4. оставлять ПЭВМ с незавершенным сеансом. При отсутствии визуального контроля за ПЭВМ, доступ к ПЭВМ должен быть заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>;

3.5. допускать посторонних лиц к ПЭВМ;

3.6. сообщать (или передавать) посторонним лицам атрибуты доступа к ресурсам ИС;

3.7. самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических средств или программного обеспечения;

3.8. открывать общий доступ к папкам на ПЭВМ;

3.9. работать на ПЭВМ при обнаружении неисправности;

3.10. самостоятельно вносить изменения в конфигурацию, размещение ПЭВМ и другие узлы ИС.

4. Ответственность

4.1. Ответственность за допуск пользователя к ресурсам и установленные ему полномочия несет руководитель структурного подразделения.

4.2. Пользователи ИС, нарушившие требования данной инструкции, несут ответственность в соответствии с действующим законодательством и внутренними организационно-распорядительными документами.

УТВЕРЖДЕНА
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ИНСТРУКЦИЯ
по организации обслуживания и ремонта технических средств в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях

1. Общие положения

Данная инструкция определяет общие принципы организации технического обслуживания и ремонта технических средств в Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях (далее – «ИС»).

инструкция регламентирует порядок обслуживания и ремонта оборудования, сопровождения программного обеспечения, устранения неисправностей программного обеспечения и технических средств ИС.

2. Обслуживание и ремонт технических средств ИС

Обслуживание технических средств ИС выполняется для обеспечения работоспособности ИС, предотвращения ее неисправностей.

При проведении технического обслуживания (далее – «ТО») и ремонта необходимо руководствоваться следующими принципами:

выполнение регламентных работ для технических средств ИС осуществляется в соответствии с технической документацией производителя;

проведение ТО и ремонт должно осуществлять подразделение или лицо, ответственное за техническое обслуживание средств вычислительной техники, а также привлекаемые специалисты (при гарантийном обслуживании);

выполнять меры по защите информации, в случае выполнения работ сторонней организацией за пределами контролируемой зоны, защищаемая информация должна быть удалена с передаваемых носителей информации;

соблюдать требования поставщика технических средств для выполнения гарантийных обязательств.

Ответственность за своевременное проведение ТО и ремонта возлагается на подразделение или лицо, ответственное за техническое обслуживание средств вычислительной техники.

3. Сопровождение программного обеспечения

При сопровождении программного обеспечения (далее - ПО) необходимо руководствоваться следующими принципами:

проводить регламентные работы по сопровождению ПО должен администратор безопасности ИС или привлекаемые специалисты в присутствии администратора безопасности ИС;

выполнять требования лицензионного соглашения на использование ПО в соответствии с законодательством Российской Федерации;

руководствоваться технической документацией производителя при сопровождении ПО;

принимать меры по исключению несанкционированного доступа к защищаемой информации при сопровождении ПО сторонними организациями;

исключить возможность изменения пользователем состава ПО.

4. Устранение неисправностей технических средств и программного обеспечения

Подразделение или лицо, ответственное за техническое обслуживание средств вычислительной техники, обеспечивает анализ и устранение неисправностей технических средств и ПО, предпринимает необходимые действия по их предупреждению.

После выявления неисправности подразделением или лицом, ответственным за администрирование ИС, а также привлекаемыми специалистами (при гарантийном обслуживании) должны выполняться необходимые работы по восстановлению работоспособности ИС, технических средств и ПО.

УТВЕРЖДЕНА
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях

1. Общие положения

1.1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях (далее – «ИС»), а также контроль за действиями пользователей и обслуживающего персонала ИС при работе с парольной защитой.

1.2. Идентификация и аутентификация пользователей в ИС осуществляется посредством использования персональных учетных записей пользователей ИС и периодически сменяемых паролей. Пароли пользователей ИС должны содержать не менее шести символов, состоять из букв и цифр, а также при смене пароля отличаться от прежнего минимум на 3 символа. Обязательная реализация идентификации и аутентификации реализуется в рамках докумена вычислительной сети Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях (далее – «организация») на автоматической основе, дополнительно реализуется программным обеспечением ИС.

1.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС, а также контроль за действиями пользователей и обслуживающего персонала ИС при работе с паролями возлагается на администратора безопасности ИС.

1.4. Временный пароль, задаваемый при создании учетной записи или смене забытого пароля, должен передаваться способом, исключающим доступ к нему других лиц, и быть изменен пользователем при первом обращении к ИС. Пароли, предустановленные производителем программного обеспечения, средства защиты информации и т.д. должны изменяться до начала их эксплуатации.

2. Порядок генерации, смены и прекращения действия и резервирования паролей

2.1. В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам ИС пользователями осуществляется периодическая (не реже раза в шесть месяцев) замена пароля в автоматическом режиме в домене вычислительной сети и по возможности в другом программном обеспечении ИС. Замена пароля осуществляется пользователем ИС самостоятельно или с привлечением администратора безопасности ИС.

2.2. В случае прекращения полномочий пользователя ИС (увольнение, переход на другую работу и т.п.) подразделение или лицо, ответственное за кадровое обеспечение организации должно уведомить об этом администратора безопасности ИС.

Администратор безопасности ИС должен произвести блокирование или удаление учетной записи пользователя ИС незамедлительно после получения такого уведомления.

2.3. Внеплановая смена паролей всех пользователей ИС должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора безопасности ИС и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

2.4. В случае компрометации личного пароля пользователя ИС проводится внеплановая смена пароля, которая выполняется лично или администратором

безопасности ИС устанавливается временный пароль.

2.5. Повседневный контроль за действиями пользователей и обслуживающего персонала ИС при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей структурных подразделений организации, администратора безопасности ИС, периодический контроль - возлагается на руководителя подразделения или лицо, ответственное за организацию обработки информации.

2.6. По решению руководителя структурного подразделения, может применяться резервирование паролей ключевых пользователей, таких, как администратор безопасности ИС, отдельных пользователей, выполняющих ключевые функции, а также пользователей, обеспечивающих работу отдельных сетевых сервисов.

2.7. Для резервирования пароля выполняются следующие действия:

пароль записывается на лист бумаги;

лист с записью пароля вкладывается владельцем в конверт. Конверт не должен допускать просмотр записи пароля на просвет. Если конверт недостаточно плотный, в него может быть вложен лист темной бумаги. Конверт заклеивается, при необходимости - опечатывается;

на конверте владелец пароля указывает свою должность, фамилию и инициалы, наименование информационного средства, доступ к которому защищается этим паролем, текущую дату и время, при необходимости – другие данные, и заверяет запись личной подписью;

конверт передается на хранение руководителю структурного подразделения или лицу, им для этого назначенным;

конверты с паролями хранятся у руководителей структурных подразделений или у администратора безопасности ИС в условиях, исключающих бесконтрольный доступ к ним. Указанные должностные лица обязаны проверять наличие конвертов с паролями, не реже раза в квартал;

при замене пароля конверт передается владельцу пароля, который уничтожает лист с резервным паролем. Новый резервный пароль подготавливается к хранению так, как указано выше;

вскрытие конверта с паролем производится по решению руководителя структурного подразделения в случае необходимости использования прав доступа его владельца в отсутствие самого владельца. О вскрытии конверта составляется акт, утверждаемый руководителем подразделения, который по окончании работы хранится в деле подразделения;

при появлении владельца пароля, после факта вскрытия конверта, пароль заменяется на новый и вновь сохраняется его копия, как описано выше.

3. Запрещается:

сообщать свой пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых пользователей ИС);

сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;

использовать учетные записи других лиц.

УТВЕРЖДЕНА
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ИНСТРУКЦИЯ
по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа

1. Общие положения

1.1. Настоящая инструкция устанавливает требования к организации учета и использования машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях (далее – «ИС»).

1.2. Учет машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа, осуществляет администратор безопасности ИС.

1.3. Все машинные носители информации, предназначенные для обработки и хранения информации ограниченного доступа (далее - МНИ), регистрируются по журналу учета и выдачи машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа (далее - Журнал) администратором безопасности ИС.

1.4. Ответственность за сохранность полученных МНИ несет пользователь ИС.

2. Учет машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа

2.1. К МНИ относятся:

съемные носители информации;

несъемные носители информации.

2.2. При обработке информации ограниченного доступа на ПЭВМ соблюдается следующий порядок учета, хранения МНИ:

2.2.1. Каждому МНИ присваивается учетный номер по Журналу. Учетный номер наносится на МНИ администратором безопасности ИС. Если невозможно маркировать непосредственно МНИ, то маркируется упаковка, в которой он хранится, или устройство, в котором установлен носитель информации.

Учетный номер состоит из двух частей АААХХХ, где:

ААА - буквенное сокращение из 3 символов (определяются администратором безопасности ИС);

ХХХ - трехзначный порядковый номер по Журналу.

2.2.2. МНИ выдаются пользователям ИС с отметкой в Журнале.

2.2.3. Хранение съемных МНИ должно осуществляться в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

2.2.4. Хранение несъемных МНИ должно осуществляться в закрываемых помещениях в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное использование, уничтожение.

2.2.5. МНИ после удаления информации ограниченного доступа с учета не снимаются. В дальнейшем эти МНИ могут использоваться для обработки и хранения информации ограниченного доступа. Если МНИ не пригодны для дальнейшего использования, они подлежат списанию и уничтожению.

2.2.6. О фактах утраты МНИ докладывается администратору безопасности ИС с внесением записи в Журнал.

2.2.7. Передача МНИ производится администратором безопасности ИС по Журналу.

2.2.8. В случае неисправности МНИ пользователь сдает его администратору безопасности ИС с внесением в Журнал записи о неисправности МНИ.

2.3. МНИ, утратившие практическое значение или пришедшие в негодность, уничтожаются.

3. Порядок уничтожения МНИ

Уничтожение МНИ производится администратором безопасности путем их физического разрушения с оформлением акта уничтожения. Перед уничтожением МНИ информация с них должна быть удалена (уничтожена, стерта и т.д.), если это возможно выполнить.

УТВЕРЖДЕНА
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ИНСТРУКЦИЯ
по организации резервного копирования информации в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях

1. Общие положения

1.1. Данная инструкция определяет порядок организации резервного копирования информации, обрабатываемой в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях (далее – «ИС»), меры поддержания непрерывности работы ИС и восстановления их работоспособности.

1.2. Задачей данной инструкции является:

определение необходимых мероприятий по защите ИС от потери информации;

определение необходимых действий по восстановлению информации ИС в случае ее потери.

1.3. Действие настоящей инструкции распространяется на администратора безопасности ИС, а в его отсутствие на замещающих его лиц и всех пользователей ИС.

1.4. Пересмотр настоящей инструкции осуществляется по мере необходимости руководителем подразделения или лицом, ответственным за обеспечение информационной безопасности.

1.5. Ответственность за обеспечение мероприятий по предотвращению инцидентов, приводящих к потере информации, возлагается на администратора безопасности ИС.

1.6. Контроль за реагированием на инциденты безопасности, приводящие к потере защищаемой информации, возлагается на руководителя подразделения или лицо, ответственное за обеспечение информационной безопасности.

2. Порядок резервирования информации

2.1. Система резервного копирования и хранения данных должна обеспечивать сохранность информации на носителях информации, не участвующих в ее обработке.

2.2. Резервное копирование данных должно осуществляться на периодической основе:

для обрабатываемой информации – не реже одного раза в неделю;

для технологической информации – не реже одного раза в 6 месяцев.

Процесс резервного копирования должен отражаться в журнале системы резервного копирования и хранения данных.

Администратор безопасности ИС должен контролировать наличие резервных копий не реже одного раза в месяц.

2.3. Носители, на которые произведено резервное копирование, должны быть учтены соответствующим образом.

2.4. Для обеспечения возможности восстановления данных резервные копии должны храниться не менее недели.

2.5. Для защиты от неисправностей носителей информации на ПЭВМ, осуществляющих обработку и хранение информации, могут применяться технические средства, основанные на RAID-технологии (кроме RAID-0), в которой применяется дублирование информации.

2.6. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование,

а также ПЭВМ должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

локальные источники бесперебойного электропитания для защиты отдельных ПЭВМ;

источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

дублирующие системы электропитания.

3. Реагирование на инцидент

3.1. Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании ИС, предоставляемых пользователям ИС, а также потеря информации.

3.2. Инцидент может произойти:

в результате непреднамеренных действий пользователей ИС;

в результате преднамеренных действий пользователей ИС или третьих лиц;

в результате нарушения правил эксплуатации технических средств ИС;

в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

3.3. В сроки, не превышающие 3 рабочих дня, администратором безопасности ИС применяются меры по восстановлению работоспособности ИС. Предпринимаемые меры в случае необходимости согласуются с руководителем подразделения, ответственного за администрирование ИС.

4. Восстановление информации из резервных копий

4.1. Работы по восстановлению данных из резервных копий производятся администратором безопасности ИС.

4.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в ИС, воздействия вредоносного программного обеспечения, ошибок программного обеспечения, ошибок пользователей ИС и аппаратных сбоев.

4.3. Восстановление программного обеспечения производится с носителей, входящих в комплект поставки, или их резервных копий в соответствии с технической документацией на данное программное обеспечение.

УТВЕРЖДЕНА
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ИНСТРУКЦИЯ
по проведению антивирусного контроля в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях

1. Общие положения

1.1. Инструкция по проведению антивирусного контроля в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях (далее – «Инструкция») предназначена для пользователей информационных систем Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях (далее – «организация»).

1.2. В целях обеспечения антивирусной защиты в информационных системах Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях органов местного самоуправления Алтайского края и подведомственных им организаций (далее – «ИС») производится антивирусный контроль.

1.3. Ответственность за поддержание установленного в Инструкции порядка возлагается на администратора безопасности ИС.

1.4. К применению в ИС допускается лицензионное антивирусное программное обеспечение.

2. Порядок проведения антивирусного контроля в ИС

2.1. Антивирусный контроль должен осуществляться на ПЭВМ в постоянном режиме.

2.2. Пользователи ИС при работе с носителями информации обязаны перед началом работы осуществить их проверку на предмет наличия вредоносного программного обеспечения.

2.3. Администратор безопасности ИС осуществляет контроль обновления антивирусных баз и функционирования антивирусной защиты информации.

2.4. Администратор безопасности ИС проводит периодическое тестирование установленного программного обеспечения на предмет наличия вирусов.

2.5. При обнаружении вредоносного программного обеспечения пользователь ИС обязан немедленно поставить в известность администратора безопасности ИС и прекратить какие-либо действия в ИС.

2.6. Администратор безопасности ИС проводит в случае необходимости лечение зараженных файлов с помощью антивирусного программного обеспечения и после этого вновь проводит антивирусный контроль.

2.7. В случае обнаружения на носителе информации вредоносного программного обеспечения, неподдающегося лечению, администратор безопасности ИС обязан запретить использование данного носителя информации, а также обязан поставить в известность руководителя подразделения или лицо, ответственное за обеспечение информационной безопасности, запретить работу в ИС и принять меры по восстановлению работоспособности ИС.

УТВЕРЖДЕНА
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

Инструкция
по обращению с носителями ключевой информации в информационных системах персональных данных Администрации Алтайского района Алтайского края, ее структурных подразделениях и подведомственных организациях

I. Термины и определения

Электронная подпись (далее - ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.
Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном Федеральным законом N 63-ФЗ "Об электронной подписи" порядке выдан сертификат ключа проверки электронной подписи.
Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.
Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.
Носитель ключевой информации (далее - ключевой носитель) - машинный носитель информации, содержащий ключ электронной подписи.

II. Общие положения

2.1. Настоящая инструкция предназначена для пользователей информационных систем персональных данных (далее - ИСПДн), использующих средства ЭП.
2.2. Инструкция содержит основные правила обращения с ключами ЭП, выполнение которых необходимо для обеспечения защиты информации при обмене электронными документами.
2.3. Работу с ключами ЭП контролирует администратор безопасности ИСПДн. Администратор безопасности ИСПДн проводит инструктаж с пользователями по правилам изготовления, хранения, обращения и эксплуатации ключей.
2.4. Владелец сертификата ключа проверки ЭП вырабатывает самостоятельно или в сопровождении администратора безопасности ИСПДн личный ключ ЭП, а также запрос на получение сертификата ключа проверки электронной подписи (в электронном виде и на бумажном носителе).
2.5. Владелец ключа ЭП несет персональную ответственность за безопасность ключей ЭП и обязан обеспечивать их сохранность, неразглашение и нераспространение, несет персональную ответственность за нарушение требований настоящей инструкции.
2.6. Запрещается оставлять без контроля ПЭВМ с незаблокированным сеансом, на котором применяется ЭП.

III. Порядок работы со средствами ЭП

2.7. Учет носителей ключевой информации осуществляет администратор безопасности ИСПДн.
2.8. Ключи ЭП изготавливаются в 2-х экземплярах: эталонная и рабочая копии. В работе используется рабочая копия ключевого носителя.
2.9. При выходе из строя носителя с ключевой информацией пользователь уведомляет об этом администратора безопасности ИСПДн. Администратор безопасности ИСПДн в присутствии пользователя изготовляет копию ключевого носителя с эталонной копии.
1.10. Не позднее, чем за 10 рабочих дней до окончания срока действия ключа ЭП, его владелец обязан выполнить все мероприятия по формированию новых ключей.
1.11. Ключевые носители хранятся в шкафах (сейфах, ящиках, хранилищах) в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.
1.12. Хранение ключевых носителей допускается в одном хранилище с другими документами и ключевыми носителями, при этом отдельно от них и в упаковке, исключающей возможность неправомерного доступа к ним.
1.13. Ключевые носители должны находиться в пределах контролируемой зоны, за исключением случаев, связанных со служебной необходимостью.
1.14. Не допускается:
- осуществлять несанкционированное администратором безопасности ИСПДн копирование ключевых носителей;
- передавать носители ключевой информации и (или) их содержимое лицам, не допущенным к ним;
- записывать на ключевые носители другую информацию.

IV. Действия при компрометации ключей ЭП

1.15. Компрометация ключа ЭП - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.
1.16. К событиям, связанным с компрометацией ключей ЭП, относятся, включая, но не ограничивая, следующие:
- потеря ключевых носителей;
- нарушение правил хранения и уничтожения;
- возникновение подозрений на утечку информации или ее искажение;
- случаи, когда нельзя установить, что произошло с ключевыми носителями.
1.17. При компрометации ключа ЭП пользователь прекращает обмен электронными документами с другими пользователями и извещает администратора безопасности ИСПДн о факте компрометации.
1.18. По факту компрометации ключей должно быть проведено служебное расследование.

V. Уничтожение ключей ЭП

1.19. Ключи ЭП должны быть выведены из действия и уничтожены в следующих случаях:
- плановая смена ключей ЭП;
- изменение данных о владельце ЭП;
- компрометация ключей;
- выход из строя ключевых носителей;
- прекращение полномочий владельца ЭП.
1.20. Уничтожение ключей ЭП может производиться путем уничтожения ключевого носителя, на котором они расположены, или путем удаления ключей без повреждения ключевого носителя.
1.21. Ключи ЭП должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия).

УТВЕРЖДЕН
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ПОРЯДОК
доступа муниципальных служащих и иных работников Администрации Алтайского района Алтайского края, ее структурных подразделений и подведомственных организаций в помещения, в которых ведется обработка персональных данных

1. Настоящий Порядок доступа служащих и работников в помещения, в которых ведется обработка персональных данных, разработан в соответствии с требованиями Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" и постановления 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".
2. Помещения, в которых ведется обработка персональных данных, должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами.
3. Персональные данные на бумажных носителях должны находиться в недоступном для посторонних лиц месте.
Бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) хранятся в шкафах, оборудованных замками.
4. Помещения, в которых ведется обработка персональных данных, запираются на ключ. Ключи от помещений ежедневно сдаются на вахту здания.
Муниципальные служащие и работники, имеющие доступ в помещения, в которых ведется обработка персональных данных, получают ключ на вахте и самостоятельно заходят в кабинеты.
5. Вскрытие и закрытие помещений, в которых ведется обработка персональных данных, производится служащими и работниками.
6. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании служебного дня гражданские служащие, имеющие право доступа в помещения, обязаны:
- убрать бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) в шкафы, закрыть шкафы;
- отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;
- закрыть окна;
- закрыть двери;
- сдать ключи от помещений, в которых ведется обработка персональных данных, на вахту здания.
7. Перед открытием помещений, в которых ведется обработка персональных данных, муниципальные служащие и работники, имеющие право доступа в помещения, обязаны:
- получить ключи от помещения, в которых ведется обработка персональных данных, на вахте здания;
- провести внешний осмотр с целью установления целостности двери и замка;
- открыть дверь и осмотреть помещение, проверить наличие и целостность замков на шкафах.
8. При обнаружении неисправности двери и запирающих устройств муниципальные служащие и работники обязаны:

- не вскрывая помещение, в котором ведется обработка персональных данных, доложить непосредственному руководителю;
- в присутствии не менее двух иных гражданских, включая непосредственного руководителя, вскрыть помещение и осмотреть его;
- составить акт о выявленных нарушениях и передать руководителю.
9. Право самостоятельного входа в помещения, где обрабатываются персональные данные, имеют только муниципальные служащие и работники, непосредственно работающие в данном помещении.
Иные служащие и граждане имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии муниципальных служащих, непосредственно работающих в данных помещениях.
10. При работе с информацией, содержащей персональные данные, двери помещений должны быть всегда закрыты.
Присутствие муниципальных служащих и граждан, не имеющих права доступа к персональным данным, должно быть исключено.
11. Техническое обслуживание компьютерной и организационной техники, сопровождение программных средств, уборка помещения, в котором ведется обработка персональных данных, а также проведение других работ осуществляются в присутствии гражданского служащего, работающего в данном помещении.
12. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на начальников структурных подразделений, обрабатывающих персональные данные.

УТВЕРЖДЕН
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

Правила
осуществления в Администрации Алтайского района Алтайского края, ее структурных подразделениях внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. В целях обеспечения соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами Администрации района (далее - Администрация), осуществляется внутренний контроль.
2. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - внутренний контроль) в Администрации района, ее структурных подразделениях организуются периодические проверки условий обработки персональных данных.
Периодические проверки условий обработки персональных данных проводятся в форме плановых и внеплановых проверок, назначенных распоряжением главы района.
3. Проверки осуществляются лицом, ответственным за организацию обработки персональных данных в Администрации, либо комиссией, образуемой распоряжением Администрации.
4. В проведении проверки не может участвовать муниципальный служащий, иной работник Администрации, заинтересованный прямо или косвенно в ее результатах.
5. Плановые проверки проводятся не реже 1 (одного) раза в год в соответствии с планом, утвержденным главой района.
6. Основанием для проведения внеплановой проверки является решение главы района либо поступившее письменное заявление гражданина или юридического лица о нарушениях правил обработки персональных данных.
7. Проведение внеплановой проверки на основании поступившего заявления о нарушениях правил обработки персональных данных организуется в течение 7 рабочих дней со дня поступления этого заявления.
8. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:
- нарушения требований Федерального закона "О защите персональных данных", иных нормативных правовых актов и локальных актов Администрации, принятых в области защиты персональных данных;
- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- осуществление мероприятий по обеспечению целостности персональных данных;

- виновность лиц, допустивших нарушения установленных требований в области защиты персональных данных.

9. Ответственный за организацию обработки персональных данных в Администрации (члены комиссии) имеет право:

- запрашивать у работников Администрации информацию, необходимую для проведения проверки;
- требовать от работников Администрации, осуществляющих обработку персональных данных, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить главе района предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить главе района предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

10. В отношении персональных данных, ставших известными лицам, проводившим проверку, должна обеспечиваться конфиденциальность персональных данных.

11. Проверка проводится в течение месяца со дня принятия решения о ее проведении.

12. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, составляется и направляется главе района заключение, подписываемое лицом, ответственным за организацию обработки персональных данных, либо председателем комиссии.

УТВЕРЖДЕН
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ПЕРЕЧЕНЬ
персональных данных обрабатываемых в Администрации Алтайского района, ее структурных подразделениях, в связи с реализацией служебных (трудовых) отношений

В связи с реализацией служебных или трудовых отношений, оказанием муниципальных услуг и осуществлением муниципальных функций в Администрации Алтайского района, ее структурных подразделениях обрабатываются следующие персональные данные:
- анкетные и биографические данные гражданина, в том числе адрес регистрации по месту жительства, адрес фактического проживания;
- паспортные данные или данные иного документа, удостоверяющего личность (включая серию, номер, дату выдачи, наименование органа, выдавшего документ), гражданство;
- сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки;
- сведения о трудовой деятельности, опыте работы, занимаемой должности, трудовом стаже, повышении квалификации и переподготовке;
- сведения о составе семьи и наличии иждивенцев, сведения о месте работы или учебы членов семьи;
- сведения о состоянии здоровья и наличии заболеваний (в случаях, установленных законом);
- сведения об отношении к воинской обязанности;
- сведения о воинском или специальном звании;
- сведения о доходах, имуществе и обязательствах имущественного характера, в том числе членов семьи;
- сведения об идентификационном номере налогоплательщика;
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
- сведения о прежних фамилии, имени, отчестве (в случае изменения);
- фотографическое изображение;
- сведения о допуске к государственной тайне;
- сведения о пребывании за границей, проживании близких родственников за границей;
- сведения о наградах и знаках отличия;
- сведения, содержащиеся в личной карточке работника, личной карточке государственного (муниципального) служащего;
- сведения о страховом номере индивидуального лицевого счета;
- сведения о наличии классного чина, дипломатического ранга, квалификационного разряда;
- сведения о наличии (отсутствии) судимости либо привлечения к административной ответственности, в том числе близких родственников;
- сведения о лицевых счетах;
- номер контактного телефона или сведения о других способах связи.

УТВЕРЖДЕНО
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
работника Администрации Алтайского района, структурного подразделения непосредственно осуществляющего обработку персональных данных, о неразглашении персональных данных

Я, _____
(фамилия, имя, отчество)
_____
(должность)
_____,
обязуюсь при исполнении своих должностных обязанностей соблюдать требования, установленные для работы с персональными данными Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными правовыми актами Администрации Алтайского района.

Обязуюсь не разглашать персональные данные, ставшие мне известными в связи с исполнением должностных обязанностей.

Обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной контракта (договора), освобождения меня от замещаемой должности и увольнения.

В соответствии со статьей 7 Федерального закона "О персональных данных" я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные, ставшие известными мне в связи с исполнением должностных обязанностей, без согласия субъекта персональных данных.

Ответственность, предусмотренная Федеральным законом "О персональных данных" и другими федеральными законами, мне разъяснена.

_____
дата

_____
подпись фамилия, имя, отчество

УТВЕРЖДЕНА
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ТИПОВАЯ ФОРМА
согласия на обработку персональных данных муниципальных служащих Администрации Алтайского района, ее структурных подразделений и иных работников

Я, _____,
(фамилия, имя, отчество)

документ, удостоверяющий личность: _____
(наименование, серия и номер)
_____
(дата выдачи, организация, выдавшая документ)

В соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" даю добровольное согласие на обработку моих персональных данных Администрации Алтайского района Алтайского края, (далее - Оператор), в целях обеспечения соблюдения Конституции Российской Федерации, трудового законодательства и иных нормативных правовых актов, содействия в прохождении муниципальной службы, обучении и продвижении по муниципальной службе, обеспечения моей безопасности и членов моей семьи, а также в целях обеспечения сохранности имущества, учета результатов исполнения должностных обязанностей и других целей осуществления трудовых отношений с Оператором, включая взаимоотношения Оператора с Федеральной налоговой службой, Пенсионным фондом России, Фондом социального страхования и подразделениями названных организаций.

Согласие дается Оператору для обработки следующих персональных данных:
фамилия, имя, отчество, пол, дата и место рождения, адрес регистрации и места фактического проживания, контактный телефон, реквизиты полисов обязательного и добровольного медицинского страхования, страховой номер индивидуального лицевого счета в Пенсионном фонде РФ (СНИЛС), идентификационный номер налогоплательщика (ИНН), паспортные данные, сведения о воинском учете, сведения о государственных наградах, семейное положение и состав семьи, сведения об образовании и трудовом стаже, о заработной плате, иных доходах, подоходном налоге, взносах в пенсионный фонд, социальных льготах, содержание служебного контракта (трудового договора), об имуществе и обязательствах имущественного характера, фотографии, сведения о состоянии здоровья в установленной форме.

Предоставляю Оператору право осуществлять любые действия (операции) по обработке моих персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор вправе использовать мои персональные данные в следующих целях:

- для формирования кадровых документов и для выполнения Оператором всех требований трудового законодательства и законодательства о муниципальной службе;
- для осуществления расчетов Оператора со мной как работником (включая передачу в финансово-кредитное учреждение (банк) для зачисления денежных средств (заработной платы, премий, материальной помощи и т.д.) на счет моей банковской карты);
- для размещения моей фотографии, фамилии, имени, отчества, должности, классного чина на доске Почета, в документах управления, на стендах в помещениях Администрации района, на официальном сайте;

- для создания и размножения (включая размещение на официальном сайте) визитных карточек и телефонных справочников с моей фамилией, именем и отчеством, рабочим телефоном для осуществления трудовой функции;

для указания моих данных (фамилия, имя, отчество, должность, рабочий телефон) в документах, подготовленных (согласованных) мною либо касающихся исполнения моих должностных обязанностей, а также в докладах, отчетах, обзорах, подготовленных по результатам деятельности Оператора и его структурных подразделений;

- для передачи в медицинское учреждение при прохождении плановой диспансеризации;

- при участии в общественных мероприятиях.

Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронные базы данных, включения в списки (реестры) и отчетные формы.

Срок хранения моих персональных данных в электронных базах данных, банках данных или хранилищах данных соответствует сроку хранения приказов по личному составу учреждения (организации) и составляет 75 (семьдесят пять) лет.

Настоящее согласие вступает в законную силу в день его подписания и действует бессрочно.

Настоящее заявление может быть отозвано мною в письменной форме в любое время по моему усмотрению.

Также подтверждаю, что ознакомлен(а) с положениями Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", права и обязанности в области защиты персональных данных мне разъяснены.

_____ _____ _____

дата подпись фамилия, имя, отчество

УТВЕРЖДЕНА
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ТИПОВАЯ ФОРМА
разъяснения субъекту персональных данных юридических
последствий отказа предоставить свои персональные данные

Мне, (Ф.И.О. полностью), разъяснены юридические последствия отказа предоставить свои персональные данные Администрации Алтайского района.

В соответствии со статьями 16, 29 Федерального закона от 02.03.2007 N 25-ФЗ "О муниципальной службе в Российской Федерации", Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденным Указом Президента Российской Федерации от 30.05.2005 N 609, определен перечень персональных данных, которые субъект персональных данных обязан предоставить Администрации Алтайского района в связи с поступлением или прохождением муниципальной службы.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений трудовой договор не может быть заключен.

_____ _____

подпись фамилия, имя, отчество

УТВЕРЖДЕНА
постановлением Администрации
Алтайского района
от 23.04.2018 года №581

ТИПОВАЯ ФОРМА ЖУРНАЛА
учета и выдачи машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа

Начат: «__» _____ 201_ г.
Окончен: «__» _____ 201_ г.
Ответственный за ведение журнала:

№ п/п	Носитель	Учетный номер носителя	Дата передачи носителя	Ф.И.О. получившего	Роспись	Примечание