АДМИНИСТРАЦИЯ ХАРЬКОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ
МУНИЦИПАЛЬНОГО РАЙОНА «РОВЕНЬСКИЙ РАЙОН»
БЕЛГОРОДСКОЙ ОБЛАСТИ
село Харьковское

07 декабря 2022 г. № 61

ПОСТАНОВЛЕНИЕ

Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Харьковского сельского поселения

В соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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", администрация Харьковского сельского поселения **постановляет:**

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Харьковского сельского поселения согласно приложению.

2. Обнародовать настоящее постановление в специально отведенных местах и разместить на официальном сайте администрации Харьковского сельского поселения муниципального района «Ровеньский район» Белгородской области в информационно-телекоммуникационной сети «Интернет».

3. Контроль за исполнением оставляю за собой.

Глава администрации
Харьковского сельского поселения **Ю.И.Снеговской**

ПРИЛОЖЕНИЕ
УТВЕРЖДЕНО
постановлением администрации
Харьковского сельского поселения
от 07.12. 2022 № 61

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Харьковского сельского поселения

1. Общие положения

2.1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в администрации Харьковского сельского поселения (далее – Администрация), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

2.1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211.

2.1.3. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн в администрации Харьковского сельского поселения проводятся в следующих целях:

1.3.1 проверка выполнения требований организационно-распорядительной документации по защите информации в администрации Харьковского сельского поселения и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.3.2 оценка уровня осведомленности и знаний работников администрации Харьковского сельского поселения в области обработки и защиты персональных данных;

1.3.3 оценка обоснованности и эффективности применяемых мер и средств защиты.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.2.1. Проверки соответствия обработки ПДн установленным требованиям в Администрации администрации Харьковского поселения разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2.2. Регулярные контрольные мероприятия проводятся Администратором АИС периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и предназначены для осуществления контроля выполнения требований в области защиты информации в администрации Харьковского сельского поселения.

2.2.3. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн администрации Харьковского сельского поселения.

2.2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.4.1 по результатам расследования инцидента информационной безопасности;

2.4.2 по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3 по решению руководителя администрации Харьковского сельского поселения.

3. Планирование контрольных мероприятий

2.3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

2.3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 сроки и этапы проведения контрольных мероприятий.

2.3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

2.4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале учета событий информационной безопасности.

2.4.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

4.2.1 описание проведенных мероприятий по каждому из этапов;

4.2.2 перечень и описание выявленных нарушений;

4.2.3 рекомендации по устранению выявленных нарушений;

4.2.4 заключение по итогам проведения внутреннего контрольного мероприятия.

2.4.3. отчет передается на рассмотрение руководству администрации Харьковского сельского поселения.

2.4.4. Общая информации о проведенном контрольном мероприятии фиксируется в Журнале учета событий информационной безопасности.

2.4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Харьковского сельского поселения (приложение 2).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

2.5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственному за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы АИС, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных администрации Харьковского сельского поселения.

2.5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

2.5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполнятся следующие проверки:

– Соответствие полномочий Пользователя правилам доступа.

– Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн.

– Соблюдение Администраторами инструкций и регламентов по обеспечению безопасности информации в администрации Харьковского сельского поселения.

– Соблюдение Порядка доступа в помещения администрации Харьковского сельского поселения, где ведется обработка персональных данных.

– Знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций.

– Знание Администраторами инструкций и регламентов по обеспечению безопасности информации в администрации Харьковского сельского поселения.

– Порядок и условия применения средств защиты информации.

– Состояние учета машинных носителей персональных данных.

– Наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер.

– Проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

– Технические мероприятия, связанные со штатным и нештатным функционированием средств защиты.

– Технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты информации.

Приложение № 1
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Харьковского сельского поселения

ПЛАН

внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Харьковского сельского поселения.

Мероприятие	**Периодичность регулярных мероприятий**	**Периодичность плановых мероприятий**	**Исполнитель**
Контроль соблюдения правил доступа к ПДн	Раз в полгода	Раз в полгода	ведущий специалист по правовой, кадровой и архивной работе администрации Харьковского сельского поселения
Контроль соблюдения режима защиты	Раз в полгода	Раз в полгода	ведущий специалист по правовой, кадровой и архивной работе администрации Харьковского сельского поселения
Контроль выполнения антивирусной политики	Раз в полгода	Раз в полгода	ведущий специалист по правовой, кадровой и архивной работе администрации Харьковского сельского поселения
Контроль выполнения парольной политики	Раз в полгода	Раз в полгода	ведущий специалист по правовой, кадровой и архивной работе администрации Харьковского сельского поселения
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Раз в полгода	Раз в полгода	ведущий специалист по правовой, кадровой и архивной работе администрации Харьковского сельского поселения
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Раз в полгода	Раз в полгода	ведущий специалист по правовой, кадровой и архивной работе администрации Харьковского сельского поселения
Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС	Раз в полгода	Раз в полгода	ведущий специалист по правовой, кадровой и архивной работе администрации Харьковского сельского

администрации Харьковского сельского поселения			поселения
Контроль обеспечения резервного копирования	Раз в полгода	Раз в полгода	ведущий специалист по правовой, кадровой и архивной работе администрации Харьковского сельского поселения
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Раз в полгода	Раз в полгода	ведущий специалист по правовой, кадровой и архивной работе администрации Харьковского сельского поселения
Поддержание в актуальном состоянии нормативно-организационных документов	Раз в полгода	Раз в полгода	ведущий специалист по правовой, кадровой и архивной работе администрации Харьковского сельского поселения
Контроль запрета на использование беспроводных соединений	Раз в полгода	Раз в полгода	ведущий специалист по правовой, кадровой и архивной работе администрации Харьковского сельского поселения

Приложение № 2
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Харьковского сельского поселения

Форма

Протокол №
контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте

_____
(наименование структурного подразделения администрации Харьковского сельского поселения)

1. Объект контроля
Указать:
наименование автоматизированного рабочего места (АРМ);
заводской (инвентарный) номер системного блока ПЭВМ АРМ;
принадлежность к подразделению;
адрес размещения АРМ.
2. Назначение объекта
Указать:
тип информации, обрабатываемой (хранимой) на АРМ;
уровень защищенности персональных данных при их обработке в информационной системе.
3. Контролируемые вопросы
Состояние организации технической защиты информации при обработке (хранении) информации ограниченного доступа.
Контроль наличия руководящих документов, инструкций, документации, регламентирующей обработку (хранение) информации ограниченного доступа:
перечня защищаемых ресурсов и уровня их конфиденциальности;
перечня лиц, обслуживающих АРМ;
перечня лиц, имеющих право самостоятельного доступа в помещение с АРМ;
перечня лиц, имеющих право самостоятельного доступа к штатным средствам АРМ и уровень их полномочий;
распоряжения о назначения комиссии для определения уровня защищенности персональных данных;
распоряжения о назначении администратора информационной безопасности;
данных по уровню подготовки персонала;
инструкции по обеспечению защиты информации, обрабатываемой на АРМ; перечня программного обеспечения;
описания технологического процесса обработки информации;
схемы информационных потоков;

технического паспорта;
матрицы доступа субъектов к защищаемым информационным ресурсам; акта установки системы активного зашумления (при наличии);
акта установки системы защиты информации от несанкционированного доступа (СЗИ НСД) (при наличии);
описания системы разграничения доступа и настроек СЗИ НСД;
инструкции администратору безопасности;
инструкции пользователю;
инструкции по антивирусному контролю;
распоряжения о допуске служащих;
распоряжения о вводе в эксплуатацию.
Контроль соответствия настройки подсистемы управления доступом, подсистемы регистрации и учета, подсистемы обеспечения целостности требованиям присвоенного класса защищенности от НСД.
В соответствии с требованиями руководящего документа "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", утвержденного решением Председателя Гостехкомиссии от 30.03.1992, в настройках подсистемы управления доступом проверяется:
наличие требований к длине и сложности пароля;
ограничение максимального срока действия пароля;
настройки блокировки учетных записей при попытках несанкционированного доступа;
наличие административных прав у пользователей;
выполнение требований мандатного разграничения прав доступа к каталогам, программам, файлам.
В настройках подсистемы регистрации и учета контролируется:
отсутствие критических ошибок и несанкционированных запусков процессов, зарегистрированных в журнале приложений;
отсутствие зарегистрированных критических системных ошибок в системном журнале;
отсутствие зарегистрированных изменений действующих политик безопасности, прав доступа, настроек системы защиты информации в журнале системы защиты информации;
возможности несанкционированного доступа к информации, аудиты отказа, зарегистрированные в журнале безопасности.
В настройках подсистемы обеспечения целостности контролируется:
соответствие программного обеспечения, установленного на АРМ, аттестационным материалам;
отсутствие программных средств разработки и отладки приложений;
наличие средств антивирусного контроля, включая срок действия лицензии и периодичность обновления антивирусных баз.
Контроль наличия лицензионного программного обеспечения, установленного в процессе проведенной аттестации по требованиям безопасности информации.
Контроль срока действия лицензии, порядка и периодичности обновления баз антивирусной программы.
Контроль наличия сетевых плат (в том числе интегрированных) и физической возможности их использования.
Контроль возможности и фактов подключения незарегистрированных магнитных и иных носителей информации.

4. Метод проведения контроля:
Экспертно-документальный

5. Средства контроля:
Программные возможности операционной системы, установленной на контролируемом АРМ.

6. Перечень документов, регламентирующих выполнение требований по обеспечению безопасности информации
Контроль проводится в соответствии с требованиями:
- Указа Президента Российской Федерации "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" от 17.03.2008 № 351;
- специальных требований и рекомендаций по технической защите конфиденциальной информации (приказ Гостехкомиссии России от 30.08.2002 № 282);
- руководящего документа "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" (решение Председателя Гостехкомиссии от 30.03.1992);
- руководящего документа "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (приказ Председателя Гостехкомиссии России от 4.06.1999 № 114);
- нормативных и руководящих документов ФСТЭК России по защите информации.

Контроль выполнили:

_____	_____	_____
должность	подпись	фамилия, инициалы
_____	_____	_____
должность	подпись	фамилия, инициалы

При проведении контроля присутствовали:

_____	_____	_____
должность	подпись	фамилия, инициалы
_____	_____	_____
должность	подпись	фамилия, инициалы

Дата проведения контроля: _____ .
(число, месяц, год)