РЕСПУБЛІКА КРИМ
БАХЧИСАРАЙСЬКИЙ РАЙОН
АДМІНІСТРАЦІЯ
ТАБАЧНЕНСЬКОГО СІЛЬСЬКОГО ПОСЕЛЕННЯ

РЕСПУБЛИКА КРЫМ
БАХЧИСАРАЙСКИЙ РАЙОН
АДМИНИСТРАЦИЯ
ТАБАЧНЕНСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ

ҚЪЫРЫМ ДЖУМХУРИЕТИ
БАГЪЧАСАРАЙ БОЛЮГИ
ТАБАЧНОЕ КОЙ
ҚЪАСАБАСЫНЫНЪ ИДАРЕСИ

ул. им Н.Г. Сотника,13, с. Табачное, Бахчисарайский район, 298430, тел./факс 98-2-17,98-3-25, tabachnoe-sovet@bahch.rk.gov.ru

РАСПОРЯЖЕНИЕ № 20/02-06

12 января 2021 г. **с. Табачное**

Об утверждении документов по обеспечению безопасности конфиденциальной информации в Администрации Табачненского сельского поселения Бахчисарайского района республики Крым

Во исполнение требований Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативно-методического документа «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденного приказом Гостехкомиссии России от 30.08.2002 № 282, приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», в целях обеспечения защиты информации и режима безопасности персональных данных работников учреждения и лиц, обращающихся за получением муниципальных услуг в Администрацию Табачненского сельского поселения Бахчисарайского района республики Крым

1. Утвердить Программу проведения инструктажа по информационной безопасности (Приложение № 1).
2. Утвердить Инструкцию по работе пользователей в автоматизированной системе и информационных системах персональных данных (Приложение № 2).
3. Контроль за исполнением настоящего распоряжения оставляю за собой.

Председатель Табачненского сельского совета-глава администрации Табачненского сельского поселения А.А. Присяжнюк

УТВЕРЖДЕНО
Приложение № 1
к распоряжению администрации
Табачненского сельского поселения
№ 20/02-06 от 12 января 2021 года

Программа проведения инструктажа по информационной безопасности

1. Общие положения

Настоящая программа разработана в соответствии с 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 РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Должностное лицо – заместитель главы администрации Табачненского сельского поселения, на которое возлагается обязанность по проведению инструктажа по информационной безопасности, назначается распоряжением от 12 января 2021 г. № 18/02-06.

Инструктаж по информационной безопасности проводится по настоящей Программе и завершается устной проверкой приобретенных работниками в результате инструктажа знаний по информационной безопасности (теоретических знаний).

Работники, показавшие по результатам инструктажа неудовлетворительные знания, к самостоятельной работе не допускаются и обязаны вновь пройти инструктаж.

Проведение инструктажа на рабочем месте регистрируется в журнале установленной формы и контрольном листе прохождения инструктажей (только при трудоустройстве) с обязательной подписью инструктирующего и инструктируемого.

2. Учебно-тематический план программы инструктажа по информационной безопасности

Цель программы: Ознакомление работников и освоение ими правил работы с персональными данными и иной конфиденциальной информации при исполнении своих должностных обязанностей.

Категория слушателей: все работники администрации Табачненского сельского поселения и лица, поступающие на работу в администрацию поселения.

Срок обучения: 60 мин.

Форма обучения: без отрыва от работы.

№п/п	Тема	Всего, мин.	В том числе		Форма контроля
			Лекции	Практик	
1.	Общие требования безопасности	10	10		Устный опрос

2.	Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей	10	10		Устный опрос
3.	Предоставление доступа работникам к информационным ресурсам, содержащим персональные данные. Разработка новых информационных	10	10		Устный опрос
4.	Инструкция по обработке персональных данных без использования средств автоматизации. Правила работы с обезличенными данными.	15	15		Устный опрос
5.	Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты. Инструкция по использованию информационных ресурсов в сети Интернет	10	10		Устный опрос
6.	Ответственность работников за невыполнение инструкции	5	5		Устный опрос
	ИТОГО:	60			

3. Содержание программы инструктажа по информационной безопасности

Тема № 1. Общие требования безопасности:

- Требования, предъявляемые к работникам;
- Термины по информационной безопасности.

Тема № 2. Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей:

- Вход работника в ИСПДн для выполнения им служебных обязанностей;
- Обязанности работников при работе в ИСПДн.

Тема № 3. Предоставление доступа работникам к информационным ресурсам, содержащим персональные данные. Разработка новых информационных ресурсов:

- Перечень правила предоставления доступа работникам в ИСПДн;
- Порядок действий при разработке новых информационных ресурсов, содержащих персональные данные.

Тема № 4. Инструкция по обработке персональных данных без использования средств автоматизации. Правила работы с обезличенными данными:

- Правила работы с персональными данными без использования средств автоматизации;
- Правила и порядок работы с обезличенными персональными данными;

Тема № 5. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты:

- Правила генерации и использования личных паролей;
- Правила организации и использования антивирусной защиты;
- Порядок действий работников при обнаружении вирусов;

Тема № 6. Ответственность работников за невыполнение инструкции.

4. Учебно-методическое обеспечение программы

1. Федеральный закон от 27.07.2016 № 152-ФЗ «О персональных данных».
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
4. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
5. Локальные нормативные акты, регулирующие правила информационной безопасности в администрации Табачненского сельского поселения.

УТВЕРЖДЕНО
Приложение № 2
к распоряжению администрации
Табачненского сельского поселения
№ 20/02-06 от 12 января 2021 года

ИНСТРУКЦИЯ
по работе пользователей в автоматизированной системе и информационных системах персональных данных

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с требованиями Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ, постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и других действующих нормативно-правовых актов Российской Федерации.

1.2. Перечень используемых по тексту сокращений. Единиц и терминов:

АИБ– администратор информационной безопасности.

АРМ – автоматизированное рабочее место.

АС ИСПДн – автоматизированная система и информационная система персональных данных.

КИ – конфиденциальная информация.

ЛВС – локальная вычислительная сеть.

НСД – несанкционированный доступ.

ПДн – персональные данные.

ПО – программное обеспечение.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в АС и ИСПДн, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Допуск пользователей для работы в АС и ИСПДн – выполнение обладателем информации или другими уполномоченными должностными лицами определенных процедур, связанных с оформлением права лица на доступ к защищаемой информации.

Доступ пользователей для работы в АС и ИСПДн – получение каждым пользователем АС и ИСПДн только письменного разрешения обладателя информации или другого уполномоченного должностного лица на право работы с информацией с учетом его служебных обязанностей.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.3. Настоящая Инструкция определяет общие требования к организации допуска пользователей для работы в АС и ИСПДн Администрации Табачненского сельского поселения Бахчисарайского района Республики Крым (далее – Администрация) при обработке (наборе, редактировании и печати) КИ и (или) ПДн, права и обязанности пользователей при работе в защищаемой АС и ИСПДн, ответственность за невыполнение предъявляемых к работе пользователей требований.

1.4. Основная цель обеспечения информационной безопасности – предотвращение несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

1.5. Методическое руководство работой пользователей, настройку параметров средств защиты, контроль работоспособности и соответствия установленным требованиям параметров настройки средств защиты, установленных на персональных компьютерах осуществляет ответственный за обеспечение информационной безопасности в Администрации (администратор информационной безопасности).

1.6. Ответственность за безопасность ПДн и соблюдение установленных правил работы при обработке ПДн возлагается на лиц, допущенных к их обработке.

2. Порядок организации допуска пользователей для работы в АС и ИСПДн

2.1. Допуск пользователей для работы в АС и ИСПДн осуществляется в соответствии со списком лиц, допущенных к обработке ПДн.

Для работы в АС и ИСПДн каждый пользователь должен получить соответствующий доступ. Под доступом понимается получение каждым пользователем АС и ИСПДн письменного разрешения на право работы с информацией с учетом его служебных обязанностей.

Устные указания о доступе кого бы то ни было к защищаемой информации в АС и ИСПДн, не имеют юридической силы и не подлежат исполнению.

2.2. Для организации доступа к работе в АС и ИСПДн с ПДн и другой КИ руководители структурных подразделений Администрации подготавливают к утверждению списки сотрудников – пользователей АС и ИСПДн. В этих списках определяются права доступа пользователей, разделы информации, на которые распространяется доступ (группы доступа), срок начала и окончания действий доступа.

2.3. Доступ пользователей в АС и ИСПДн организует АИБ при получении оформленного соответствующим образом разрешения.

3. Общие принципы работы пользователя

3.1. Работа пользователей в системе разрешена на закреплённых за ними компьютерами, в определенное время и только с разрешенными программами и сетевыми ресурсами.

3.2. Вход в систему в обязательном порядке осуществляется на основе ввода (по запросу системы) имени, присвоенного при первичной регистрации АИБом и ввода личного пароля, требования к которому установлены в «Политике использования паролей». Пароль не может быть сообщён другому лицу за исключением случаев,

предусмотренных в «Политике использования паролей». В случае отказа системы в идентификации пользователя, либо не подтверждения личного пароля следует немедленно обратиться к АИБу.

3.3. Все автоматизированные рабочие места, установленные в Администрации, имеют унифицированный набор установленного программного обеспечения, определенный в «Перечне, разрешенного к использованию программного обеспечения». Самостоятельная установка программного обеспечения на автоматизированные рабочие места запрещена. Установка и удаление любого программного обеспечения производится только уполномоченными сотрудниками в порядке, установленном в Администрации. Установка и использование игровых программ запрещено.

3.4. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется уполномоченными сотрудниками. Самовольное перемещение средств вычислительной техники является нарушением персональной ответственности за сохранность переданных сотруднику во временное пользование средств автоматизации. Перемещение любых средств вычислительной техники производится в порядке, установленном в Администрации. Изменение конструкции, конфигурации средств вычислительной техники запрещено.

3.5. Для постоянного хранения и обработки КИ и ПДн разрешается использовать исключительно каталоги, определенные АИБом или администратором АС и ИСПДн. Использование отчуждаемых носителей в данных целях запрещено.

3.6. Пользователю разрешается обрабатывать информацию в рамках определенных полномочий доступа, обрабатывать информацию с грифом конфиденциальности выше заявленного при регистрации запрещено.

3.7. Пользователю запрещается осуществлять попытки НСД к ресурсам системы и других пользователей; пытаться подменять функции АИБа по перераспределению времени работы и полномочий доступа к ресурсам компьютера.

3.8. При обнаружении неисправности в работе АРМ, элементов информационной системы, средств защиты пользователю запрещается продолжать работать на АРМ. Об обнаруженных неисправностях необходимо сообщить АИБу или администратору АС и ИСПДн.

4. Обеспечение безопасности персональных данных при использовании сети Интернет

4.1. Доступ к сети Интернет предоставляется в соответствии с должностными обязанностями сотрудника с целью получения оперативной и достоверной информации, необходимой для выполнения должностных обязанностей. Разрешение и изменение доступа к ресурсам Интернет (в том числе к внешним почтовым сервисам) производится в порядке, установленном в Администрации.

4.2. Пользователям, имеющим право доступа в Интернет запрещается:

- пересылка документов, содержащих КИ, в т.ч. ПДн по сети Интернет, электронной почте или с использованием клиентов службы мгновенного обмена сообщениями (ICQ и т.п.);
- использование сети Интернет для развлечения, в т.ч. посещения сайтов «социальных сетей» и сервисов, и получения информации, не относящейся к функциональным обязанностям пользователя;
- доступ к сети Интернет и электронной почте не со своего рабочего места с

использованием данных своей учетной записи;

- предоставление доступа к сети Интернет с использованием данных своей учетной записи другим лицам;
- публикация своего адреса электронной почты в электронных каталогах и на поисковых машинах сети Интернет;
- подписка по электронной почте на различные рекламные материалы, листы рассылки, электронные журналы и т.п., не связанные с выполнением пользователем функциональных обязанностей;
- открытие (запуск на выполнение) файла, полученного из сети Интернет или по электронной почте, без предварительной проверки его антивирусным ПО.

5. Порядок проведения антивирусного контроля

5.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по электронной почте, интернет-ресурсам, а также информация на съемных носителях (флешках, CD-ROM, внешних дисках и т.п.).

5.2. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.), либо на наличие заражения съемного носителя, пользователь самостоятельно или вместе с ответственным за обеспечение безопасности информации (администратором информационной безопасности) должен провести внеочередной антивирусный контроль своей рабочей станции.

5.3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в Администрации;
- провести лечение или уничтожение зараженных файлов.

5.4. Пользователям запрещается:

- отключать средства антивирусной защиты информации во время работы.
- открывать сомнительные электронные письма (необходимо удаление), ссылки, сайты, источники переноса информации.

6. Обеспечение безопасности конфиденциальной информации и персональных данных при использовании съемных носителей

6.1. Пользователям запрещается:

- хранить съемные носители с КИ и ПДн вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с КИ и ПДн из служебных помещений для работы с ними на дому и т. д.

6.2. При отправке или передаче КИ и ПДн адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей КИ и ПДн для непосредственной передачи адресату осуществляется только с письменного

разрешения руководителя структурного подразделения.

7. Обеспечение безопасности перед началом обработки конфиденциальной информации и персональных данных

7.1. Перед началом обработки КИ и ПДн необходимо убедиться в том, что:

- в помещении, в котором ведется работа с КИ и ПДн, отсутствуют посторонние лица;
- технические средства, с использованием которых осуществляется обработка КИ и ПДн, и средства защиты КИ и ПДн находятся в исправном состоянии;
- используемые в работе носители КИ и ПДн не повреждены;
- к КИ и ПДн не был осуществлен НСД.

8. Обеспечение безопасности во время обработки конфиденциальной информации и персональных данных

8.1. Во время обработки конфиденциальной информации и персональных данных необходимо обеспечить:

- недопущение нахождения в помещении, в котором ведется работа с персональными данными, посторонних лиц;
- недопущение воздействия на технические средства, с использованием которых осуществляется обработка персональных данных, способного нарушить их функционирование;
- постоянный контроль за соблюдением условий эксплуатации средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- недопущение несанкционированного доступа к персональным данным;
- конфиденциальность персональных данных.

8.2. Во избежание получения НСД к информационным ресурсам АРМ сотрудника устанавливается хранитель экрана, который автоматически включается через 10 минут отсутствия работы на данном компьютере, при этом выход из режима хранителя экрана возможен только при введении идентификационных данных пользователя. При необходимости отлучиться от рабочего места пользователь обязан принудительно запустить хранитель экрана посредством комбинации клавиш «Windows + L» либо другим доступным способом.

9. Обеспечение безопасности при завершении обработки конфиденциальной информации и персональных данных

9.1. После завершения сеанса обработки персональных данных необходимо обеспечить:

- исключение возможности несанкционированного проникновения или нахождения посторонних лиц в помещении, в котором размещены технические средства, используемые для обработки конфиденциальной информации и персональных данных, и ведется работа с конфиденциальной информации и персональными данными;
- работоспособность средств защиты информации, функционирующих при отсутствии лиц, допущенных к обработке конфиденциальной информации и персональных данных.

10. Порядок действий в случае обнаружения фактов нарушения безопасности персональных данных

10.1. При нарушении порядка предоставления КИ и ПДн пользователям информационной системы необходимо приостановить их предоставление.

10.2. При обнаружении НСД к КИ или ПДн необходимо немедленно прекратить несанкционированный доступ.

10.3. При модификации или уничтожения КИ и ПДн, вследствие НСД к ним необходимо обеспечить их незамедлительное восстановление.

10.4. В случае обнаружения фактов несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности КИ и ПДн или другим нарушениям, приводящим к снижению уровня защищенности КИ и ПДн необходимо произвести фиксацию данных фактов, служебное расследование и заключение по данным фактам, разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

10.5. Обо всех случаях нарушения безопасности КИ и ПДн необходимо немедленно поставить в известность главу Администрации и произвести служебное расследование.

11. Права пользователей

11.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам АС и ИСПДн, присвоенными АИБом данному пользователю. При этом для хранения файлов, содержащих ПДн, разрешается использовать только специально выделенные каталоги, а также соответствующим образом учтенные внешние носители.

12. Ответственность пользователей

12.1. Пользователь отвечает за правильность включения и выключения АРМ, входа в систему и все действия при работе в АС и ИСПДн.

12.2. Пользователь АС и ИСПДн несет персональную ответственность за соблюдение установленных требований во время работы в ЛВС.

12.3. Пользователи АС и ИСПДн, виновные в нарушении законодательства Российской Федерации о защите прав собственности и охраняемых по закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно распорядительными документами Администрации.

12.4. Ответственность за допуск пользователя к ЛВС и установленные ему полномочия несет АИБ.

13. Заключительные положения

13.1. Кроме выполнения указанных выше требований при работе с персональными данными пользователь обязан соблюдать положения Политики информационной безопасности Администрации.

13.2. Проверка и пересмотр настоящего Руководства осуществляются в следующих случаях:

- при пересмотре межотраслевых и отраслевых требований обеспечения безопасности персональных данных;

- при внедрении новой техники и (или) технологий;
- по результатам анализа материалов расследования нарушений требований законодательства об обеспечении безопасности персональных данных;
- по требованию представителей органов контроля в сфере обеспечения безопасности персональных данных.

13.3. По всем возникающим вопросам при работе в АС и ИСПДн необходимо обращаться к АИБу.

С распоряжением ознакомлены:

Сухань О.П.
Бурундукова Г.А.
Ломоносова В.Ю.
Кугмир А.В.
Полядник А.В.