РЕСПУБЛІКА КРИМ
БАХЧИСАРАЙСЬКИЙ РАЙОН
АДМІНІСТРАЦІЯ
КАШТАНІВСЬКОГО СІЛЬСЬКОГО
ПОСЕЛЕННЯ

РЕСПУБЛИКА КРЫМ
БАХЧИСАРАЙСКИЙ РАЙОН
АДМИНИСТРАЦИЯ
КАШТАНОВСКОГО СЕЛЬСКОГО
ПОСЕЛЕНИЯ

ҚЪЫРЫМ ДЖУМХУРИЕТИ
БАГЪЧАСАРАЙ БОЛЮГИ
КАШТАНЫ КОЙ
ҚЪАСАБАСЫНЫНЪ ИДАРЕСИ

298413, Республика Крым, Бахчисарайский район, село Каштаны, ул.Виноградная,4 тел(06554)51323 kashtany-sovet@bahch.rk.gov.ru

РАСПОРЯЖЕНИЕ № 02-08/146

от «22» июня 2020 года **с.Каштаны**

Об утверждении Положения об организации и проведении работ в администрации Каштановского сельского поселения по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных

В соответствии с Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», в целях обеспечения безопасности персональных данных в Администрации Каштановского сельского поселения Бахчисарайского района Республики Крым,

ПРИКАЗЫВАЮ:

1. Утвердить Положение об организации и проведении работ в администрации Каштановского сельского поселения по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных согласно приложению.
2. Данное распоряжение подлежит размещению на официальном сайте Каштановского сельского поселения http://kashtanovskoe-sp.ru.
3. Контроль за выполнением настоящего распоряжения оставляю за собой.

Председатель Каштановского сельского совета – главы администрации Каштановского сельского поселения Бахчисарайского района Республики Крым **В.Э.Григорян**

УТВЕРЖДЕНО
распоряжением администрации
Каштановского сельского поселения
№ 02-08/146 от «22» июня 2020 года

Положение об организации и проведении работ в администрации Каштановского сельского поселения по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных

1. Общие положения

1.1. Данное «Положение об организации и проведении работ в администрации Каштановского сельского поселения по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации, порядок контроля ИСПДн при остановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок обслуживания компьютерного оборудования и установки системного программного обеспечения, порядок охраны и допуска посторонних лиц в помещения ИСПДн.

2. Порядок работы сотрудников администрации Каштановского сельского поселения в ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн

Настоящий порядок определяет действия сотрудников администрации Каштановского сельского поселения ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Допуск пользователей для работы на персональной электронной вычислительной машине (далее – ПЭВМ) осуществляется в соответствии со списком лиц допущенных к работе в ИСПДн.

2.2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации.

2.3. Пользователь несет ответственность за правильность включения и выключения ПЭВМ, входа в систему и все действия при работе в ИСПДн.

2.4. Вход пользователя в систему осуществляться по персональному паролю.

2.5. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на ПЭВМ. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

2.6. Каждый сотрудник администрации Каштановского сельского поселения , участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и *обязан*:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на ПЭВМ;
- хранить в тайне свой пароль (пароли), менять свой пароль (пароли) в соответствии с Инструкцией по организации парольной защиты в локально-вычислительных сетях;
- хранить в установленном порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);
- выполнять требования Инструкции по организации антивирусной защиты в полном объеме.

Немедленно известить заведующего информационно-компьютерным отделом в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данной защищенной ПЭВМ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПЭВМ, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на ПЭВМ технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

Пользователю ПЭВМ категорически *запрещается*:

- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения ПЭВМ;
- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра ПЭВМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации

3.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации.

3.2. К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные носители конфиденциальной информации.

3.3. Постоянный пользователь *обязан* осуществлять периодическое резервное копирование конфиденциальной информации.

3.4. По окончанию работы с конфиденциальными документами (ПДн) на ПЭВМ, пользователь обязан создавать резервную копию конфиденциальных документов на зарегистрированный носитель (ЖМД, ГМД, CD, DVD – диски, USB накопитель, другие), создавая тем самым резервный электронный архив конфиденциальных документов.

3.5. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение ответственному по защите информации управления.

3.6. Перед резервным копированием пользователь обязан проверить электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель) на отсутствие вирусов.

3.7. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.

3.8. Запрещается запись посторонней информации на электронные носители (ЖМД, ГМД, CD-ROM, USB накопитель и другие) резервной копии.

3.9. Порядок создания резервной копии:

- вставить в ПЭВМ зарегистрированный электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель, другие) для резервного копирования;

- выбрать необходимый каталог (файл) для создания резервного архива;

- нажать по выбранному каталогу (файлу) правой кнопкой манипулятора и в появившемся меню выбрать пункт «Добавить в архив…»;

- на вкладке «Общие» нажать на кнопку «Обзор» и в появившемся окне перейти на электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель), после чего нажать кнопку «Открыть»;

- на вкладке «Общие» в поле «Имя архива» ввести имя архива следующего вида: «Имя каталога (файла) резервного копирования. Дата архивирования. Имя пользователя.;

- нажать кнопку «ОК».

3.10. Ответственность за проведение резервного копирования в ИСПДн в соответствии с требованиями настоящего Положения возлагается на пользователя.

4. Порядок контроля ИСПДн при остановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения

условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий

4.1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения техническими средствами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

4.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в администрации Каштановского сельского поселения и учета требований по защите информации в разрабатываемых плановых и распорядительных документах;
- выявление демаскирующих признаков объектов ИСПДн;
- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;
- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;
- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

4.3. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных (далее – ОБ ПДн);
- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;
- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- эффективность применения организационных и технических мероприятий по защите информации;
- устранение ранее выявленных недостатков.

4.4. Основными видами технического контроля на объекте организации, являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

4.5. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и

требований по защите информации, заведующий информационно-компьютерным отделом администрации района докладывает главе администрации района о допущенных нарушениях, для принятия им решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по их устранению. Результаты контроля защиты информации оформляются актами.

4.6. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию главы администрации Каштановского сельского поселения проводится расследование.

Для проведения расследования назначается комиссия. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования глава администрации Каштановского сельского поселения принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

4.7. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты.

4.8. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год

4.9. Обследование объектов информатизации проводится с целью определения основных и вспомогательных технических средств и систем требованиям по защите информации.

4.10. В ходе обследования проверяется:

- соответствие класса обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;
- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;
- наличие электробытовой, радио и телевизионной аппаратуры, которые могут способствовать возникновению каналов утечки информации;
- выполнение требований предписаний на эксплуатацию на основные технические средства и системы по их размещению относительно вспомогательных технических средств и систем, организации электропитания и заземления;
- соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в техническом паспорте;
- выполнение требований по защите автоматизированных систем от несанкционированного доступа;
- выполнение требований по антивирусной защите.

4.11. Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, других нарушений и способов возникновения каналов утечки информации необходимо:

- тщательно осмотреть мебель, сувениры (особенно иностранного производства), оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы и т.д.;

5. Правила организации антивирусной защиты.

Организация антивирусной защиты в автоматизированных системах администрации Каштановского сельского поселения осуществляется в соответствии с Инструкцией по организации антивирусной защиты в автоматизированных информационных системах.

6. Правила организации парольной защиты.

Организация парольной защиты в администрации Каштановского сельского поселения осуществляется в соответствии с соответствующей Инструкцией.

7. Заключительные положения.

7.1. Требования настоящего Положения обязательны для всех сотрудников администрации Каштановского сельского поселения, обрабатывающих конфиденциальную информацию.

7.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

7.3. Нарушения, связанные с выполнением требований руководящих документов по информационной безопасности, применению средств защиты информации и разграничения доступа, использованию технического, информационного и программного обеспечения ИСПДн, по степени их опасности делятся на нарушения первой, второй и третьей категории.

7.4. К нарушениям первой категории относятся нарушения, повлекшие за собой разглашение (утечку) защищаемых сведений, утрату содержащих их машинных носителей информации и машинных документов, уничтожение (искажение) информационного и программного обеспечения, выведение из строя технических средств.

7.5. К нарушениям второй категории относятся нарушения, в результате которых возникают предпосылки к разглашению (утечке) защищаемых сведений или утрате содержащих их машинных носителей информации и машинных документов, уничтожению (искажению) информационного и программного обеспечения, выведению из строя технических средств.

7.6. Остальные нарушения относятся к нарушениям третьей категории.