



РЕСПУБЛИКА КРИМ  
БАХЧИСАРАЙСЬКИЙ РАЙОН  
АДМІНІСТРАЦІЯ  
КАШТАНІВСЬКОГО СІЛЬСЬКОГО  
ПОСЕЛЕННЯ

РЕСПУБЛИКА КРЫМ  
БАХЧИСАРАЙСКИЙ РАЙОН  
АДМИНИСТРАЦИЯ  
КАШТАНОВСКОГО СЕЛЬСКОГО  
ПОСЕЛЕНИЯ

КЪЫРЫМ ДЖУМХУРИЕТИ  
БАГЪЧАСАРАЙ БОЛЮГИ  
КАШТАНЫ КОЙ  
КЪАСАБАСЫНЫЪ ИДАРЕСИ

298413, Республика Крым, Бахчисарайский район, село Каштаны, ул.Виноградная,4 тел(06554)51324

## РАСПОРЯЖЕНИЕ № 02-09/159

от «22» июня 2020 года

с.Каштаны

Об утверждении инструкции по информационной безопасности пользователя информационных систем, компьютерной техники, локальных вычислительных сетей, мобильных устройств администрации Каштановского сельского поселения Бахчисарайского района Республики Крым

В целях обеспечения защиты информации в администрации Бахчисарайского района Республики Крым, в соответствии Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», с приказом №17 ФСТЭК России от 11.02.2013 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», во исполнение Протокола заседания Совета по защите информации при Главе Республики Крым от 10.04.2017, распоряжения администрации Бахчисарайского района Республики Крым от 23.08.2017 № 87 «Об утверждении Политики информационной безопасности администрации Бахчисарайского района Республики Крым»,

### ПРИКАЗЫВАЮ:

1. Утвердить инструкцию по информационной безопасности пользователя информационных систем, компьютерной техники, локальных вычислительных сетей, мобильных устройств администрации Каштановского сельского поселения Бахчисарайского района Республики Крым согласно Приложению.
2. Контроль за исполнением распоряжения оставляю за собой.

Председатель Каштановского сельского совета –  
главы администрации Каштановского  
сельского поселения Бахчисарайского района  
Республики Крым



В.Э.Григорян

## УТВЕРЖДЕНА

распоряжением администрации  
Каштановского сельского поселения  
№ 02-08/159 от «22» июня 2020 года

### **Инструкция по информационной безопасности пользователя информационных систем, компьютерной техники, локальных вычислительных сетей, мобильных устройств администрации Каштановского сельского поселения Бахчисарайского района Республики Крым**

#### **Определения**

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);

**Сведения конфиденциального характера** – сведения, определенные законодательством и (или) нормативно-правовыми актами администрации Каштановского сельского поселения Бахчисарайского района Республики Крым как сведения, не подлежащие разглашению;

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами;

**Мобильное устройство** – мобильный телефон, планшет, смартфон, ноутбук.

**Устройство хранения информации** – магнитный диск HDD, твердотельный диск SSD, USB-накопитель (флеш-накопитель), карта памяти (в том числе в составе мобильного устройства, фотокамеры, видеокамеры), оптический диск (CD-R, DVD-R, CD-RW, DVD-RW).

**Корпоративная мобильная связь** - совокупность услуг мобильной связи, предоставляемых оператором мобильной связи на основании договора, заключенного с администрацией района, и используемых сотрудниками администрации Каштановского сельского поселения.

**Компрометация** - хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с конфиденциальной информацией, в результате которых информация может стать доступной несанкционированным лицам и (или) процессам.

#### **Обозначения и сокращения**

Администратор ИБ	– администратор информационной безопасности
АРМ	– автоматизированное рабочее место
ИС	– информационная система
НСД	– несанкционированный доступ
ПДн	– персональные данные



СЗИ	– система защиты информации
СрЗИ	– средство защиты информации
ФСБ России	– Федеральная служба безопасности Российской Федерации
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю

## **1. Общие положения**

1.1. Инструкция по информационной безопасности пользователя информационных систем, компьютерной техники, локальных вычислительных сетей, мобильных устройств администрации Бахчисарайского района Республики Крым (далее – Инструкция) определяет функциональные обязанности, права и ответственность пользователей информационных систем и локальных вычислительных сетей администрации Каштановского сельского поселения Бахчисарайского района Республики Крым (далее – Пользователя).

1.2. Настоящая Инструкция подготовлена в соответствии с требованиями нормативно-методических документов ФСТЭК России и ФСБ России по защите информации, обрабатываемой с использованием средств автоматизации.

## **2. Обязанности пользователя**

2.1. Пользователь обязан:

2.1.1. Хранить в тайне информацию, ставшую ему известной во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки защищаемой информации немедленно информировать ответственного за организацию обработки информации и персональных данных, администратора ИБ.

2.1.2. Знать и выполнять правила работы с СрЗИ, используемыми на персональных компьютерах в соответствии с Инструкциями, требованиями, регламентирующими функционирование установленных СрЗИ.

2.1.3. Хранить в тайне свой пароль доступа в ИС администрации Каштановского сельского поселения Бахчисарайского района Республики Крым (далее – администрация поселения), а также информацию о системе защиты, установленной в администрации поселения.

2.1.4. Использовать для обработки информации служебного пользования только учтенные технические средства (компьютеры, мобильные устройства, устройства хранения информации).

2.1.5. Сообщать о необходимости обновления антивирусных баз администратору ИБ.

2.1.6. Немедленно ставить в известность администратора ИБ:

- в случае утери носителя с конфиденциальной информацией и/или при подозрении компрометации личных ключей, паролей или иной информации;
- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров

печатаей) на аппаратных средствах АРМ или иных фактов совершения попыток НСД;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств.

2.1.7. В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных СрЗИ ставить в известность администратора ИБ.

2.1.8. Оперативно докладывать администратору ИБ о случаях возникновения внештатных ситуаций и аварийных ситуаций.

2.1.9. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

2.1.10. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИС администрации поселения. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

2.2. В случае увольнения пользователь обязан вернуть все документы и материалы, относящиеся к деятельности организации. В том числе: отчеты, инструкции, служебную переписку, списки работников, компьютерные программы, пароли, съемные носители информации, технические средства (компьютеры, мобильные устройства), а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности администрации поселения, полученные в течение срока работы.

2.3. Уборка помещений должна производиться под контролем пользователь, имеющего доступ в помещение и постоянно в нем работающего.

2.5. Вынос технических средств, на которых проводилась обработка защищаемой информации, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с ответственным за организацию обработки информации и персональных данных запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

2.6. АРМ, используемые для работы с защищаемой информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора.

2.7. Пользователю категорически запрещается:

- передавать кому бы то ни было, устно или письменно, защищаемую информацию;

- использовать защищаемую информацию при подготовке открытых публикаций, докладов, научных работ и т.д.;

- выполнять работы с документами, содержащими защищаемую информацию, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения ответственного за организацию обработки информации и персональных данных;



- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие защищаемую информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами, содержащими защищаемую информацию;
- использовать компоненты программного и аппаратного обеспечения ИС администрации поселения в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию технических средств администрации поселения в части установки программных и аппаратных средств;
- осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра свое АРМ, не активизировав средства защиты информации от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность администратора ИБ;
- использовать посторонние технические средства - компьютеры, мобильные устройства и прочее), находящиеся за пределами администрации поселения в служебных целях (осуществлять доступ к корпоративной почте, системе электронного документооборота и другим информационным системам, в том числе удаленный доступ с помощью специальных программ);
- подключать посторонние технические средства - компьютеры, мобильные устройства, Wi-Fi маршрутизаторы, точки доступа, коммутаторы, устройства хранения к корпоративной локальной вычислительной сети администрации района.
- подключать посторонние технические средства - мобильные устройства, устройства хранения информации к компьютерам администрации поселения;
- распаковывать и запускать на компьютере файлы, скачанные из сети Интернет, или полученные из незнакомых источников и по электронной почте;
- работать на компьютере без установленного антивирусного программного обеспечения, с устаревшими базами.
- временно отключать антивирусное программное обеспечение;
- хранить информацию конфиденциального характера и информацию, содержащую персональные данные, в сетевых папках и облачных сервисах;
- посещать посторонние сайты, социальные сети (кроме пользователей, которые работают с социальными сетями при исполнении ими служебных обязанностей);
- пользоваться личной почтой, а также личными облачными сервисами в служебных целях;
- пользоваться служебной почтой в личных целях.

### 3. Права пользователя

3.1. Пользователь имеет право:

3.1.1. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.2. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимых для надлежащего исполнения своих обязанностей.

#### **4. Ответственность пользователя**

4.1. Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также нормативных документов в области защиты информации. За разглашение защищаемой информации, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

4.2. За разглашение защищаемой информации, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

#### **5. Учет и контроль**

5.1. Администратор ИБ организует и ведет учет всех машинных съемных носителей информации, используемых для обработки и накопления персональных данных. Учет носителей информации осуществляется соответствии с распоряжением администрации Каштановского сельского поселения Бахчисарайского района Республики Крым.

5.2. Администратор ИБ осуществляет контроль пользователей информационных систем. Приоритет проверок – объекты, использующие сетевые технологии обработки информации и запись информации на съемные носители (USB-накопители, оптические диски, мобильные устройства).