



РЕСПУБЛИКА КРИМ  
БАХЧИСАРАЙСКИЙ РАЙОН  
АДМІНІСТРАЦІЯ  
УГЛІВСЬКОГО СІЛЬСЬКОГО ПОСЕЛЕННЯ

РЕСПУБЛИКА КРЫМ  
БАХЧИСАРАЙСКИЙ РАЙОН  
АДМИНИСТРАЦИЯ  
УГЛОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ

КЪЫРЫМ ДЖУМХУРИЕТИ  
БАГЪЧАСАРАЙ БОЛЮГИ  
УГЛОВЕ КОЙ  
КЪАСАБАСЫНЫНЪ ИДАРЕСИ

## Постановление

30 апреля 2019г.

№ 131

*Об утверждении Политики  
информационной безопасности  
администрации Угловского сельского поселения  
Бахчисарайского района Республики Крым*

В соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", в целях систематизации работ по защите информационных ресурсов в администрации Угловского сельского поселения Бахчисарайского района Республики Крым,

### ПОСТАНОВЛЯЮ:

1. Утвердить Политику информационной безопасности администрации Угловского сельского поселения Бахчисарайского района Республики Крым (Приложение).
2. Контроль за выполнением настоящего распоряжения возложить на заместителя главы администрации Угловского сельского поселения

**Председатель Угловского сельского совета –  
глава администрации  
Угловского сельского поселения**

**Н.Н. Сосницкая**

Приложение  
к постановлению администрации  
Угловского сельского поселения  
Бахчисарайского района  
Республики Крым  
от «30» апреля 2019 г. №131

**ПОЛИТИКА**  
**информационной безопасности администрации**  
**Угловского сельского поселения Бахчисарайского района Республики Крым**

1. Общие положения

1.1. Политика информационной безопасности (далее – Политика) администрации Угловского сельского поселения Бахчисарайского района Республики Крым (далее - администрация поселения) определяет цели и задачи системы обеспечения информационной безопасности (далее – ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется администрация поселения в своей деятельности.

1.2. Основными целями Политики администрации поселения являются защита информации, организация и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении полномочий по решению вопросов местного значения и полномочий по осуществлению отдельных государственных полномочий, переданных органам местного самоуправления, указанных в Уставе муниципального образования Угловское сельское поселение Бахчисарайского района Республики Крым.

1.3.Общее руководство обеспечением ИБ администрации поселения осуществляет заместитель главы администрации поселения, на которого возложены обязанности по вопросам технической защиты информации. Ответственное лицо по информационной безопасности осуществляет контроль за соблюдением требований ИБ и несет ответственность за организацию мероприятий по обеспечению ИБ (далее – администратор ИБ). Ответственность за функционирование автоматизированной системы (далее – АС) администрации поселения несет специалист, чьими должностными обязанностями являются вопросы информатизации, обслуживание компьютерной техники и локальной вычислительной сети администрации поселения (далее – системный администратор).

Должностные обязанности администратора ИБ и системного администратора закрепляются в должностных инструкциях.

Муниципальные служащие обязаны соблюдать порядок обращения со сведениями ограниченного доступа, носителями ключевой информации и другой защищаемой информацией, соблюдать требования Политики и других документов ИБ.

1.4. Политика администрации района направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий муниципальных служащих, технических сбоев, неправильных

технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Наибольшими потенциальными возможностями для нанесения ущерба администрации района располагают ее муниципальные служащие. Действия муниципальных служащих могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне администрации района) либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией муниципальных служащих и их способностью к адекватным действиям в нештатной ситуации.

Для противодействия угрозам ИБ в администрации поселения на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя.

Разработанная на основе прогноза Политика и в соответствии с ней построенная система управления ИБ (далее – СУИБ) является наиболее правильным и эффективным способом минимизации рисков нарушения ИБ для администрации поселения. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий муниципальных служащих.

#### 1.5. Задачами Политики являются:

- описание организации системы управления информационной безопасностью в администрации поселения;

- определение структуры Политики ИБ администрации поселения как следующих составных частей:

  - система мероприятий по реализации антивирусной защиты;

  - система мероприятий по ведению учетных записей;

  - система мероприятий по предоставлению доступа к информационному ресурсу;

  - система мероприятий по использованию информационного ресурса в рамках существующих информационных систем;

  - система мероприятий по использованию паролей;

  - система мероприятий по защите автоматизированных рабочих мест (далее – АРМ);

  - система мероприятий работы с носителями информации ограниченного доступа;

  - определение порядка сопровождения информационных систем (далее – ИС) администрации района.

1.6. Область действия Политики распространяется на все органы администрации района и обязательна для исполнения всеми муниципальными

служащими. Положения настоящей Политики применимы для использования в правовых актах администрации поселения, а также в договорах и иных документах.

1.7. Политика вводится в действие и признается утратившей силу правовым актом администрации района.

Изменения в Политику вносятся правовым актом администрации поселения. Инициатором внесения изменений в Политику является ответственное лицо по информационной безопасности, который выполняет функции администратора ИБ.

Плановая актуализация Политики производится ежегодно и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация Политики производится в обязательном порядке в следующих случаях: при изменении политики Российской Федерации в области ИБ, правовых актов в области защиты информации; при изменении нормативных документов (инструкций, положений, руководств), касающихся ИБ администрации района; при происшествии и выявлении нарушений ИБ, способных причинить ущерб администрации поселения.

Ответственность за актуализацию Политики ИБ (плановую и внеплановую), контроль за исполнением ее требований несет ответственное лицо по информационной безопасности, которое выполняет функции администратора ИБ.

## 2. Термины и определения

Автоматизированная система – система, состоящая из муниципальных служащих администрации поселения и комплекса средств автоматизации ее деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор ИБ – муниципальный служащий или группа муниципальных служащих администрации поселения, осуществляющих контроль за обеспечением защиты информации в локальной вычислительной сети, а также осуществляющих организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления несанкционированного доступа к защищаемой информации.

Администратор сети – муниципальный служащий или группа муниципальных служащих администрации поселения, осуществляющих непосредственную организацию и выполнение работ по созданию (модернизации), техническому обслуживанию и управлению (администрированию) информационной управляющей локальной вычислительной сети (далее - ЛВС), включая технические аспекты ИБ.

Актив – информация, представляющая ценность для администрации поселения.

Анализ риска – систематическое использование информации для определения источников и оценки риска.

Аудит ИБ – процесс проверки выполнения установленных требований по обеспечению ИБ. Может проводиться как самой организацией (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита.

Аутентификация – проверка принадлежности субъекту доступа

предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Владелец информационных активов – муниципальный служащий администрации поселения, получивший на основании соответствующего распорядительного документа права обладателя информации, обрабатываемой в информационной системе.

Внутренняя сеть – внутренний участок корпоративной сети, отделенный от внешней сети (сети Интернет) и демилитаризованной зоны (DMZ) межсетевым экраном. Внутренняя сеть объединяет производственные, тестовые, административные сети и сети разработчиков.

Доступ к информации – возможность получения информации и ее использования.

Доступность – доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Доступность информации – состояние информации, характеризующееся способностью АС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защищенный канал передачи данных – логические и физические каналы сетевого взаимодействия, защищенные от прослушивания потенциальными злоумышленниками средствами шифрования данных (средствами VPN), либо путем их физической изоляции и размещения на охраняемой территории.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов администрации поселения в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками муниципальных служащих, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.) или преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов администрации района.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения производственных задач структурных подразделений администрации поселения. В администрации района используются различные типы информационных систем для решения производственных, управленческих, учетных и других задач.

Информационная среда – совокупность информационно-телекоммуникационной системы администрации поселения, процессов, источников и потребителей информации, обслуживающего муниципальных служащих и

пользователей информационных систем, обеспечивающая автоматизацию производственных процессов администрации поселения.

Информационно-телекоммуникационная система – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники, а также информационные системы, обеспечивающие автоматизацию процессов администрации поселения, и средства защиты информации.

Информационные активы – информационные системы, информационные средства, информационные ресурсы.

Информационные ресурсы – совокупность содержащейся в базе данных (далее - БД) информации и обеспечивающих ее обработку информационных технологий, используемая в рабочих процессах администрации поселения.

Информационные средства – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные ин и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация – актив, который, подобно другим активам администрации поселения, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Инфраструктура открытых ключей – технологическая инфраструктура и сервисы, обеспечивающие безопасность информационных и коммуникационных систем на основе использования криптографических алгоритмов и сертификатов ключей подписей.

Инцидент ИБ – действительное, предпринимаемое или вероятное нарушение ИБ, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов администрации поселения.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

Код аутентификации электронного сообщения – данные, используемые для установления подлинности и контроля целостности электронного сообщения.

Конфиденциальность – доступ к информации только санкционированных пользователей.

Корпоративная сеть – объединение информационных систем, компьютерного, телекоммуникационного и офисного оборудования всех органов администрации поселения, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.

Критичная информация – информация, нарушение доступности, целостности либо конфиденциальности которой может оказать негативное влияние на функционирование органов администрации поселения, нанести администрации

последствия материальный или иной ущерб.

Криптопровайдер – программный или программно-аппаратный модуль, реализующий алгоритмы шифрования.

Локальная вычислительная сеть – группа персональных компьютеров (далее – ПК), а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран (далее – МЭ) – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав корпоративной сети, а также между корпоративной сетью и внешними сетями (сетью Интернет).

Менеджмент риска – скоординированные действия по руководству и управлению учреждением в отношении риска.

Мониторинг ИБ – постоянное наблюдение за объектами, влияющими на обеспечение ИБ, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть АС или ее часть, информационные технологические процессы администрации поселения, информационные услуги администрации поселения и пр.

Несанкционированный доступ к информации (далее – НСД) – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Обработка риска – процесс выбора и осуществления мер по модификации риска.

Операционная система (далее – ОС) – системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью ПК.

Орган администрации поселения – структурное подразделение администрации поселения с самостоятельными функциями, задачами и ответственностью, закрепленными в Положении о нем.

Остаточный риск – риск, остающийся после обработки риска.

Оценивание риска – процесс сравнения оцененного риска с данными критериями риска для определения значимости риска.

Оценка риска – общий процесс анализа риска и оценивания риска.

Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

Периметральное средство защиты информации (далее – СЗИ) – шлюз информационной безопасности, обеспечивающий межсетевое экранирование и защиту данных, пересылаемых по открытым каналам связи (шифрование), а также фильтрацию вредоносного программного обеспечения (далее – ПО) и блокирование внешних атак.

Политика ИБ – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в учреждении для обеспечения его ИБ.

Пользователь ЛВС – муниципальный служащий администрации поселения, а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в корпоративной сети в установленном порядке и получившие права на доступ к

ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.

Принятие риска – решение принять риск.

Программное обеспечение – совокупность системных и прикладных программ, установленных на сервере или персональном компьютере.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – запись, которая включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в ОС (сети, БД, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления БД, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название органа администрации, телефоны, адрес его электронной почты и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Сервер – выделенный компьютер, имеющий разделяемые ресурсы, выполняющий определенный перечень задач и предоставляющий пользователям ЛВС ряд сервисов.

Сетевые (информационные) сервисы – сетевые приложения, предоставляющие различные виды сервисов для внутренних и внешних пользователей корпоративной сети, включая DNS, FTP, HTTP, Telnet, и другие.

Система менеджмента информационной безопасности (СМИБ) – та часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и совершенствовании ИБ.

Системный администратор – муниципальный служащий администрации района, занимающийся сопровождением АС, отвечающий за функционирование локальной сети администрации поселения и персональных компьютеров.

Список контроля доступа (ACL) – правила фильтрации сетевых пакетов, настраиваемые на маршрутизаторах и МЭ, определяющие критерии фильтрации и действия, производимые над пакетами.

Собственник – лицо или организация, которые имеют утвержденные обязательства по менеджменту для контроля производства, разработки, поддержки, использования и безопасности активов. Термин «собственник» не означает, что лицо действительно имеет какие-либо права собственности на актив.

Средства криптографической защиты информации – средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

Угрозы информационным данным – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения



или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Управление информационной безопасностью – совокупность целенаправленных действий, осуществляемых в рамках Политики ИБ в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению ИБ администрации поселения при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность информации ограниченного доступа при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца ключа подписи, а также установить отсутствие искажения информации в электронном документе.

VPN (Virtual Private Network) – «виртуальная частная сеть»: технология и организация систематической удаленной связи между wybranymi группами узлов в крупных распределенных сетях.

### 3. Обозначения и сокращения

АРМ – автоматизированное рабочее место

АС – автоматизированная система

БД – база данных

ИБ – информационная безопасность

ИОК – инфраструктура открытых ключей

ИС – информационная система

НСД – несанкционированный доступ

ОС – операционная система

ПО – программное обеспечение

СЗИ – средство защиты информации

СУИБ – система управления информационной безопасностью

ПК – персональный компьютер

### 4. Системы мероприятий ИБ администрации поселения

#### 4.1. Назначение систем мероприятий ИБ

Системы мероприятий ИБ администрации поселения – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в администрации поселения.

Под системами мероприятий ИБ понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Системы мероприятий ИБ относятся к административным мерам ее обеспечения и определяют стратегию администрации поселения в области ИБ.

Системы мероприятий ИБ регламентируют эффективную работу средств защиты информации. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Системы мероприятий ИБ реализуются посредством административно-организационных мер, физических и программно-технических средств и определяют архитектуру системы защиты.

Все документально оформленные решения, формирующие системы мероприятий, должны быть утверждены председателем Угловского сельского совета – главой Угловского сельского поселения.

#### 4.2. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются следующие:

4.2.1. Постоянный и всесторонний анализ информационного пространства администрации поселения с целью выявления уязвимостей информационных активов;

4.2.2. Своевременное обнаружение проблем, потенциально способных повлиять на ИБ администрации поселения, корректировка моделей угроз и нарушителя;

4.2.3. Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей администрации поселения, а также повышать трудоемкость технологических процессов обработки информации;

4.2.4. Контроль эффективности принимаемых защитных мер;

4.2.5. Персонификация и адекватное разделение ролей и ответственности между муниципальными служащими администрации поселения, исходя из принципа персональной ответственности за совершаемые операции.

#### 4.3. Соответствие систем мероприятий действующему законодательству

Правовую основу систем мероприятий составляют федеральные законы и другие законодательные акты, определяющие права и ответственность граждан, органов государственной власти и органов местного самоуправления в сфере безопасности, а также нормативные, отраслевые и ведомственные документы по вопросам безопасности информации, утвержденные органами исполнительной власти Российской Федерации и Республики Крым в пределах их компетенции.

#### 4.4. Ответственность за реализацию систем мероприятий ИБ

Ответственность за разработку мер и контроль обеспечения защиты информации несёт администратор ИБ.

Ответственность за реализацию мероприятий возлагается: в части, касающейся

разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на системного администратора; в части, касающейся доведения правил систем мероприятий до муниципальных служащих администрации поселения, а также иных лиц (предусмотренных п. 1.4.) – на администратора ИБ; в части, касающейся исполнения правил систем мероприятий, – на каждого муниципального служащего администрации поселения, согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей Политики.

#### 4.5. Порядок подготовки муниципальных служащих по вопросам ИБ и допуска их к работе

Организация обучения муниципальных служащих администрации поселения в области ИБ возлагается на администратора ИБ. Подписи муниципальных служащих об ознакомлении заносятся в Журнал проведения инструктажа по ИБ (Приложение 1 к Политике). Обучение муниципальных служащих администрации поселения правилам обращения с информацией ограниченного доступа проводится путем: проведения администратором ИБ инструктивных занятий с муниципальными служащими, принимаемыми на работу в администрацию поселения; самостоятельного изучения муниципальным служащим документов, реализующих Политику ИБ администрации поселения.

Допуск муниципальных служащих к работе с информационными ресурсами администрации поселения осуществляется только после их ознакомления с системами мероприятий ИБ, а также после ознакомления пользователей с Инструкцией по информационной безопасности пользователя, а также иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований систем мероприятий ИБ подтверждается подписями муниципальных служащих в Журнале проведения инструктажа по ИБ.

Допуск муниципальных служащих к работе с информацией ограниченного доступа администрации поселения осуществляется после ознакомления с Инструкциями по обращению с носителями информации ограниченного распространения. Правила допуска к работе с информационными ресурсами лиц, не являющихся муниципальными служащими администрации поселения, определяются на договорной основе с лицами или с организациями, представителями которых эти лица являются.

#### 4.6. Защищаемые информационные ресурсы администрации поселения

Различаются следующие категории информационных ресурсов, подлежащих защите в администрации поселения:

Информация ограниченного доступа (конфиденциальная) – информация, определенная в соответствии с федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", предусмотренная Перечнем сведений конфиденциального характера.

Публичная информация – информация, получаемая из публичных источников (публикации в средствах массовой информации, теле- и радиовещание и т.д.), а также информация, предназначенная для размещения на внешних публичных ресурсах.

Открытая информация – информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная в результате деятельности администрации поселения, которую запрещено относить к конфиденциальной на основании российского законодательства. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности администрации поселения или имеющая принципиальное значение для имиджа администрации поселения.

Конфиденциальная информация представляет собой сведения ограниченного доступа, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

Подходы к решению проблемы защиты информации в администрации поселения состоят в исключении неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования рабочих процессов администрации поселения.

Для этого в администрации поселения выполняются следующие мероприятия: определяется порядок работы с документами, носителями и др., содержащими сведения ограниченного распространения; устанавливается круг лиц и порядок доступа к подобной информации; вырабатываются меры по контролю обращения с документами, содержащими сведения ограниченного распространения; включаются в трудовые договоры с муниципальными служащими обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Подписка о неразглашении конфиденциальной информации совершается при заключении трудового договора, который подписывается каждым муниципальным служащим при приеме на работу в администрацию района. Защита информации ограниченного доступа, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых администрацией поселения с другими организациями.

#### 4.7. Организация СУИБ администрации поселения

СУИБ администрации поселения предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ администрации района.

Для успешного функционирования СУИБ администрации поселения должны быть реализованы следующие процессы: определение и уточнение области действия СУИБ и выбор подхода к оценке рисков ИБ; определение и уточнение области действия СУИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью администрации района, а также оценки репутационных и правовых рисков деятельности администрации поселения; анализ и

оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов и производственных процессов; выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ; принятие администрацией поселения остаточных рисков и решения о реализации и эксплуатации/совершенствовании СУИБ. Остаточные риски ИБ должны быть соотнесены с рисками деятельности администрации поселения и оценено их влияние на достижение целей ее деятельности.

#### 4.8. Реализация СУИБ администрации поселения

В СУИБ реализуются следующие процессы: разработка плана обработки рисков ИБ; реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СУИБ; реализация программ по обучению и осведомленности ИБ; обнаружение и реагирование на инциденты безопасности; обеспечение непрерывности деятельности и восстановления после прерываний.

На этапе планирования определяется набор подходов к управлению рисками в ИБ, методология управления ими, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков.

На этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. Администрацией поселения принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне либо минимизировать. После этого разрабатывается и внедряется план обработки рисков.

На этапе проверки отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.

На этапе действия по результатам непрерывного мониторинга и проводимых проверок выполняются необходимые корректирующие действия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку Политики и методологии управления рисками, а также плана обработки рисков.

#### 4.9. Методы оценивания информационных рисков

Оценка информационных рисков администрации района выполняется по следующим основным этапам: идентификация и количественная оценка информационных ресурсов, значимых для работы администрации поселения; оценивание возможных угроз; оценивание существующих уязвимостей; оценивание эффективности средств обеспечения ИБ.

Предполагается, что значимые для производственного процесса уязвимые информационные ресурсы администрации поселения подвергаются риску, если по отношению к ним существуют какие-либо угрозы.

При этом информационные риски зависят от: показателей ценности информационных ресурсов; вероятности реализации угроз для ресурсов; эффективности существующих или планируемых средств обеспечения ИБ.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков

становится возможным выбрать средства, обеспечивающие желаемый уровень ИБ администрации поселения.

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например, учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса администрации поселения.

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями: привлекательностью ресурса, показатель используется при рассмотрении угрозы от умышленного воздействия со стороны человека; возможностью использования ресурса для получения дохода, показатель используется при рассмотрении угрозы от умышленного воздействия со стороны человека; техническими возможностями реализации угрозы, показатель используется при умышленном воздействии со стороны человека; степенью легкости, с которой уязвимость может быть использована.

#### 4.10. Порядок предоставления доступа к информационному ресурсу

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей Политикой.

Каждому муниципальному служащему администрации поселения, допущенному к работе с конкретным информационным ресурсом администрации поселения, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

В случае производственной необходимости некоторым муниципальным служащим могут быть сопоставлены несколько уникальных имен (учетных записей).

#### 4.11. Порядок создания (продления) учетной записи пользователя

Процедура регистрации (создания учетной записи), также продления срока действия временной учетной записи пользователя для муниципального служащего администрации поселения инициируется заявкой руководителя органа администрации, в котором работает данный муниципальный служащий, по форме (Приложение 2 к настоящей Политике).

В заявке указываются: должность (с полным наименованием органа администрации), фамилия, имя и отчество муниципального служащего; основание для регистрации учетной записи (номер распоряжения о принятии на работу в администрацию района или реквизиты иного документа, определяющего необходимость предоставления муниципальному служащему доступа к информационным ресурсам администрации поселения).

Заявку подписывает руководитель органа администрации поселения.

Заявка согласовывается с администратором ИБ и передается системному администратору.

Системный администратор рассматривает представленную заявку и совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к сетевым ресурсам администрации поселения, таких, как право регистрации на АРМ муниципального служащего и пользования корпоративной электронной почтой.

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.

Назначение минимальных прав в ИС администрации поселения, а также присвоение начального пароля производится администратором ИБ при согласовании заявки на предоставление (изменение) прав доступа пользователя к информационным ресурсам.

#### 4.12. Порядок предоставления (изменения) полномочий пользователя.

Процедура предоставления (или изменения) прав доступа пользователя к ресурсам администрации поселения инициируется заявкой муниципального служащего по форме (Приложение 3 к настоящей Политике).

В заявке указываются: должность, фамилия, имя и отчество муниципального служащего; имя пользователя (учетной записи) данного муниципального служащего; наименование информационного актива (системы, ресурса), к которому необходим допуск (или изменение полномочий пользователя); полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на конкретных информационных ресурсах ИС) с указанием разрешенных видов доступа к ресурсу (ролей).

Заявку подписывает руководитель органа администрации поселения, в котором числится муниципальный служащий согласно штатному расписанию, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного муниципального служащего к необходимым ресурсам ИС администрации поселения для решения им указанных задач.

Администратор ИБ и системный администратор рассматривают представленную заявку и вносят необходимые изменения в списки полномочий пользователей соответствующих информационных ресурсов.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

#### 4.13. Порядок удаления учетной записи пользователя

При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение муниципального служащего) учетная запись должна немедленно блокироваться. При этом руководитель органа администрации поселения, эксплуатирующего ИС, должен быть уведомлен письменно о наличии или отсутствии в ИС механизма автоматического блокирования учетной записи пользователя.

В случае наступления прекращения срока действий пользователя необходимо подать заявку на блокирование учетной записи муниципального служащего по форме (Приложение 4 к настоящей Политике) не позднее, чем за сутки до момента прекращения срока действия полномочий пользователя.

В заявке указываются: должность муниципального служащего, фамилия, имя и отчество муниципального служащего; имя пользователя (учетной записи) данного

муниципального служащего; дата прекращения полномочий пользователя.

Заявку подписывает руководитель органа администрации поселения.

Администратор ИБ рассматривает представленную заявку и производит блокировку учетной записи пользователя.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

#### 4.14. Порядок хранения исполненных заявок

Исполненные заявки хранятся у администратора ИБ в течение 1 года с момента окончания предоставления доступа к информационному ресурсу администрации поселения.

Копии заявок передаю системному администратору.

Они могут впоследствии использоваться: для восстановления полномочий пользователей после аварий в ИС администрации поселения; для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам системы при разборе конфликтных ситуаций; для проверки системным администратором правильности настройки средств разграничения доступа к ресурсам системы.

4.15. Порядок подключения пользователей (создание, изменение и прекращение действия учетных записей) к системе электронного документооборота (далее - СЭД) определяется Регламентом, утвержденным Оператором СЭД. Назначение на должность, изменения должности, увольнение с должности муниципальных служащих обязательно сопровождается подачей соответствующих заявлений Оператору СЭД.

#### 4.16. Система мероприятий ведения учетных записей

Настоящая система мероприятий ИБ определяет основные правила присвоения учетных записей пользователям информационных активов администрации поселения.

Регистрационные учетные записи подразделяются на: пользовательские, предназначенные для идентификации/аутентификации пользователей информационных активов администрации поселения; системные, используемые для нужд ОС; служебные, предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов администрации района назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

Запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо (например, (посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале событий ОС, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются ОС и должны использоваться только в случаях, предписанных документацией на ОС.

Служебные регистрационные учетные записи используются только для



запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

#### 4.17. Система мероприятий по использованию паролей

Настоящая система мероприятий определяет основные правила обращения с паролями, используемыми для доступа к информационным активам администрации поселения. Положения системы мероприятий закрепляются в Инструкции по организации парольной защиты в АС.

#### 4.18. Система мероприятий реализации антивирусной защиты

Настоящая система мероприятий определяет основные правила для реализации антивирусной защиты в администрации поселения.

Положения системы мероприятий закрепляются в Инструкции по проведению антивирусного контроля в АС.

#### 4.19. Система мероприятий защиты АРМ

4.19.1. Настоящая система мероприятий определяет основные правила и требования по защите информации ограниченного доступа администрации поселения от неавторизованного доступа, утраты или модификации.

4.19.2. Во время работы с информацией ограниченного доступа должен предотвращаться ее просмотр не допущенными к ней лицами;

4.19.3. При любом оставлении рабочего места рабочая станция должна быть заблокирована, съемные машинные носители, содержащие информацию ограниченного доступа, заперты в помещении, шкафу или ящике стола, или в сейфе;

4.19.4. Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа;

4.19.5. Муниципальные служащие получают доступ к ресурсам вычислительной сети после ознакомления с документами, регулирующими защиту персональных данных и утвержденными администрацией поселения согласно занимаемой должности;

4.19.6. Доступ к компонентам ОС и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратору ИБ и системному администратору. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей;

4.19.7. Доступ к корпоративной информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей;

4.19.8. Пользователям запрещается устанавливать ПО на компьютеры без согласования с системным администратором;

4.19.9. Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неразрешенного ПО;

4.19.10. Техническое обслуживание должно осуществляться только на основании зарегистрированного обращения пользователя к системному администратору;

4.19.11. Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя;

4.19.12. Дистанционное техническое обслуживание должно осуществляться только со специально выделенных АРМ, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться;

4.19.13. При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и должны использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений;

4.19.14. Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации, в том числе в составе АРМ, допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ;

4.19.15. ПО должно устанавливаться со специальных сетевых ресурсов или съемных носителей, маркированных в соответствии с лицензионным соглашением с его правообладателем;

4.19.16. Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию регламентированы;

4.19.17. АРМ, на которых предполагается обрабатывать информацию ограниченного доступа, должны быть закреплены за соответствующим муниципальным служащим администрации поселения. Запрещается использование указанных АРМ другими пользователями без согласования с системным администратором. При передаче указанного АРМ другому пользователю должна производиться гарантированная очистка диска (форматирование);

4.19.18. Системный администратор отказывает в устранении проблемы, вызванной наличием на рабочем месте ПО или оборудования, установленного или настроенного пользователем с нарушением действующей процедуры.

#### 4.20. Порядок сопровождения ИС администрации поселения

Обеспечение ИБ на стадиях жизненного цикла (далее – ЖЦ) ИС должно осуществляться на всех его стадиях, автоматизирующих технологические процессы, с учетом всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг соответствующих органов администрации поселения. Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводится при участии администратора ИБ и системного администратора. Порядок разработки и внедрения ИС должен контролироваться системным администратором.

При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами, входящими в группу ГОСТ 34 «Стандарты

информационной технологии».

Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при участии администратора ИБ.

На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз: неверной формулировки требований к ИС; выбора неадекватной модели ЖЦ ИС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников; принятия неверных проектных решений; внесения разработчиком дефектов на уровне архитектурных решений; внесения разработчиком недокументированных возможностей в ИС; неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к ИС; разработки некачественной документации; сборки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований; неверного конфигурирования ИС; приемки ИС, не отвечающей требованиям заказчика; внесения недокументированных возможностей в ИС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

Привлекаемые для разработки и (или) производства средств и систем защиты ИС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством Российской Федерации.

При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, содержащая, в том числе, описание защитных мер, предпринятых разработчиком в отношении угроз ИБ.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС, и их компонентов, касающихся безопасности разработки, безопасности поставки, эксплуатации, поддержки ЖЦ, включая описание модели ЖЦ, оценки уязвимости. Данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

В договор (контракт) о поставке ИС и их компонентов включаются положения по сопровождению поставляемых модулей на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику, должна быть рассмотрена возможность приобретения полного комплекта рабочей документации на модуль для обеспечения последующего сопровождения ИС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой цены, администрация района должна провести анализ влияния угрозы невозможности сопровождения ИС и их компонентов на обеспечение непрерывности технологического процесса.

На стадии эксплуатации должна быть обеспечена защита от следующих угроз: умышленное несанкционированное раскрытие, модификация или уничтожение информации; неумышленная модификация или уничтожение информации;

недоставка или ошибочная доставка информации; отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения. На стадии сопровождения должна быть обеспечена защита от угроз: внесение изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей; невнесение разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб администрации поселения, и информации, используемой средствами обеспечения ИБ, из постоянной памяти или с внешних носителей.

Требования ИБ должны включаться во все договоры и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ ИС.

#### 4.21. Профилактика нарушений системы мероприятий ИБ

Под профилактикой нарушений системы мероприятий ИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в администрации поселения и проведение разъяснительной работы по ИБ среди пользователей администрации поселения.

Проведение в ИС администрации поселения регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность с точностью до периода тестирования. Контрольное тестирование функций СЗИ может быть частичным или полным и должно проводиться с установленной в ИС администрации поселения степенью периодичности.

Задача предупреждения в ИС администрации поселения возможных нарушений ИБ решается по мере наступления следующих событий: включение в состав ИС администрации поселения новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС администрации поселения; изменение конфигурации программных и технических средств ИС администрации поселения (изменение конфигурации ПО рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС администрации поселения; появление сведений о выявленных уязвимых местах в составе ОС и/или ПО технических средств, используемых в ИС администрации поселения.

Администратор ИБ, в том числе используя рекомендации организации, специализирующейся в области ИБ и имеющей соответствующие сертификаты Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК), собирает и анализирует информацию о выявленных уязвимых местах в составе ОС и/или ПО относительно ИС администрации поселения. Источниками подобного рода сведений могут служить официальные издания и публикации в средствах массовой информации, общественных объединений и других организаций, специализирующихся в области защиты информации.

Администратор ИБ, в том числе используя рекомендации организации, специализирующейся в области ИБ и имеющей соответствующие сертификаты ФСТЭК, организует периодическую проверку СЗИ ИС администрации поселения путем моделирования возможных попыток осуществления НСД к защищаемым информационным ресурсам.

Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных в составе СЗИ ИС администрации района средств и функций защиты. По результатам профилактических работ, проводимых в ИС администрации поселения, необходимо сделать соответствующие записи в Журнале проверки исправности и технического обслуживания (Приложение 5 к Политике).

Плановая разъяснительная работа по правилам системы мероприятий ИБ, а также инструктаж муниципальных служащих администрации поселения по соблюдению требований нормативных и регламентных документов по ИБ, принятых в администрации района, проводятся администратором ИБ по мере необходимости.

Внеплановая разъяснительная работа по правилам системы мероприятий ИБ, а также инструктаж муниципальных служащих администрации поселения по соблюдению требований нормативных и регламентных документов по ИБ, принятых в администрации поселения, проводятся при пересмотре системы мероприятий ИБ, при возникновении инцидента нарушения правил системы мероприятий.

Прием на работу муниципальных служащих должен сопровождаться ознакомлением их с правилами и требованиями системы мероприятий.

#### 4.22. Ликвидация последствий нарушения системы мероприятий ИБ

Администратор ИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС администрации поселения, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым информационным ресурсам ИС администрации поселения необходимо уведомить администратора ИБ и системного администратора и далее следовать их указаниям.

Действия администратора ИБ и системного администратора при признаках нарушения системы мероприятий ИБ регламентируются следующими документами: Политикой ИБ; Инструкцией по информационной безопасности пользователя; должностной инструкцией администратора ИБ; должностной инструкцией системного администратора.

После устранения нарушения необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС администрации поселения (Приложение 6 к Политике), а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий (Приложение 7 к Политике).

#### 4.23. Ответственность нарушителей систем мероприятий ИБ

Ответственность за выполнение правил систем мероприятий безопасности несет каждый муниципальный служащий администрации поселения в рамках своих служебных обязанностей и полномочий.

**Заместитель главы администрации  
Угловского сельского поселения**

**Е.С. Стравкина**

Приложение 1  
к Политике  
информационной безопасности  
администрации Угловского сельского  
поселения Бахчисарайского района  
Республики Крым

**ЖУРНАЛ**  
проведения инструктажа по информационной безопасности  
в администрации Угловского сельского поселения Бахчисарайского района  
Республики Крым

Начато «\_\_»\_\_\_\_\_20\_\_ г.  
Окончено«\_\_»\_\_\_\_\_20\_\_ г.  
Кол-во листов \_\_\_\_\_  
Срок хранения \_\_\_\_\_

<b>№ п/ п</b>	<b>Дата инструктажа</b>	<b>ФИО сотрудника прошедшего инструктаж</b>	<b>Должность сотрудника прошедшего инструктаж</b>	<b>Инструктаж провел (ФИО - должность)</b>	<b>Подпись сотрудника, подтверждающая проведение инструктажа</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>



Приложение 2  
к Политике  
информационной безопасности  
администрации Угловского сельского  
поселения Бахчисарайского района  
Республики Крым

СОГЛАСОВАНО

Отдел организационной и кадровой работы

\_\_\_\_\_  
(должность) (подпись) (расшифровка подписи)  
«\_\_\_» \_\_\_\_\_ 20\_\_ г.

Администратор информационной безопасности

\_\_\_\_\_  
(должность) (подпись) (расшифровка подписи)  
«\_\_\_» \_\_\_\_\_ 20\_\_ г.

ЗАЯВЛЕНИЕ № \_\_\_\_\_  
на создание (продление) учетной записи пользователя

Прошу создать (продлить) учетную запись пользователя:

Наименование органа администрации	
Ф.И.О. муниципального служащего, должность, телефон	
Ф.И.О. непосредственного руководителя, должность, телефон	

Муниципальный служащий приступает к работе с: «\_\_\_» \_\_\_\_\_ 20\_\_ г.  
по «\_\_\_» \_\_\_\_\_ 20\_\_ г. (указывается при необходимости)

Обоснование служебной  
необходимости: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
(Ф.И.О. руководителя подразделения администрации) (подпись)  
«\_\_\_» \_\_\_\_\_ 20\_\_ г.

С правилами работы в информационной системе администрации поселения

ознакомлен(а)

\_\_\_\_\_ (Ф.И.О. муниципального служащего) (подпись)  
«\_\_» \_\_\_\_\_ 20\_\_ г.

Выполнено: \_\_\_\_\_  
(назначенное имя пользователя) (адрес корпоративной почты)

Системный администратор \_\_\_\_\_  
(Подпись) (Ф.И.О.)

Системное время: \_\_\_\_ чч \_\_\_\_ мм

Дата: «\_\_» \_\_\_\_\_ 20\_\_ г.

Приложение 3  
к Политике  
информационной безопасности  
администрации Угловского сельского  
поселения Бахчисарайского района  
Республики Крым

СОГЛАСОВАНО

Администратор информационной безопасности

\_\_\_\_\_  
(должность) (подпись) (расшифровка подписи)  
«\_\_» \_\_\_\_\_ 20\_\_ г.

ЗАЯВЛЕНИЕ № \_\_\_\_\_

На изменение полномочий пользователя

Прошу изменить полномочия по работе с информационным ресурсом:

Наименование органа администрации	
Ф.И.О. муниципального служащего, должность, телефон	
Имя в системе (указывается, если есть)	
Ф.И.О. непосредственного руководителя, должность, телефон	
Наименование информационного ресурса	
Старые полномочия (если были)	
Новые полномочия	

Изменения вступают в силу с: «\_\_» \_\_\_\_\_ 20\_\_ г.  
по «\_\_» \_\_\_\_\_ 20\_\_ г. (указывается при необходимости)

Обоснование служебной

необходимости: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_  
(Ф.И.О. руководителя подразделения администрации) (подпись)  
«\_\_» \_\_\_\_\_ 20\_\_ г.

С правилами работы в информационной системе администрации поселения

ознакомлен(а)

\_\_\_\_\_  
(Ф.И.О. муниципального служащего)

\_\_\_\_\_  
(подпись)

«\_\_» \_\_\_\_\_ 20\_\_ г.

Выполнено: \_\_\_\_\_

(назначенное имя пользователя)

\_\_\_\_\_  
(адрес корпоративной почты)

Системный администратор \_\_\_\_\_

(Подпись)

\_\_\_\_\_  
(Ф.И.О.)

Системное время: \_\_\_\_ чч \_\_\_\_ мм

Дата: «\_\_» \_\_\_\_\_ 20\_\_ г.

Приложение 4  
к Политике  
информационной безопасности  
администрации Угловского сельского  
поселения Бахчисарайского района  
Республики Крым

СОГЛАСОВАНО

Отдел организационной и кадровой работы

\_\_\_\_\_  
(должность) (подпись) (расшифровка подписи)  
«\_\_» \_\_\_\_\_ 20\_\_ г.

Администратор информационной безопасности

\_\_\_\_\_  
(должность) (подпись) (расшифровка подписи)  
«\_\_» \_\_\_\_\_ 20\_\_ г.

ЗАЯВЛЕНИЕ № \_\_\_\_\_

На блокировку учетной записи пользователя

Прошу заблокировать учетную запись пользователя:

Наименование органа администрации	
Ф.И.О. муниципального служащего, должность, телефон	
Имя в системе	
Ф.И.О. непосредственного руководителя, должность, телефон	

Срок действия полномочий прекратить с: «\_\_» \_\_\_\_\_ 20\_\_ г.

Основание

блокировки: \_\_\_\_\_

\_\_\_\_\_  
(Ф.И.О. руководителя подразделения администрации) (подпись)  
«\_\_» \_\_\_\_\_ 20\_\_ г.

Пользователь заблокирован

Системный администратор \_\_\_\_\_  
(Подпись) (Ф.И.О.)

Системное время: \_\_\_\_ чч \_\_\_\_ мм

Дата: « \_\_\_\_ » \_\_\_\_\_ 20 \_\_ г.

Приложение 5  
к Политике  
информационной безопасности  
администрации Угловского сельского  
поселения Бахчисарайского района  
Республики Крым

**ЖУРНАЛ**

проверки исправности и технического обслуживания информационных систем и  
компьютерной техники  
администрации Угловского сельского поселения Бахчисарайского района  
Республики Крым

Начато «\_\_» \_\_\_\_\_ 20\_\_ г.  
Окончено «\_\_» \_\_\_\_\_ 20\_\_ г.  
Кол-во листов \_\_\_\_\_  
Срок хранения \_\_\_\_\_

Дата	Наименование ИС или оборудования	Вид ТО. Должность, фамилия проводившего проверку или ТО ИС или оборудования	Подпись	Выявленные недостатки и неисправности, замечания	Отметка об устранении замечаний, недостатков, неисправностей. Дата, должность, фамилия, Подпись
1	2	3	4	5	6



Приложение 6  
к Политике  
информационной безопасности  
администрации Угловского сельского  
поселения Бахчисарайского района  
Республики Крым

АКТ №\_\_\_ от «\_\_\_»\_\_\_\_\_20\_\_ г.  
о факте нарушения информационной безопасности  
и принятых мерах по восстановлению работоспособности ИС

Мною, \_\_\_\_\_  
(Ф.И.О.)

\_\_\_\_\_  
(должность)

в присутствии \_\_\_\_\_  
(Ф.И.О.)

\_\_\_\_\_  
(должность)

«\_\_\_»\_\_\_\_\_20\_\_ г. выявлен факт нарушения информационной безопасности:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_,  
\_\_\_\_\_  
\_\_\_\_\_

Нарушение устранено «\_\_\_»\_\_\_\_\_20\_\_ г.

\_\_\_\_\_  
(Ф.И.О.)

\_\_\_\_\_  
(должность)

Принятые меры:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(должность лица, составившего акт)

(подпись)

(расшифровка подписи)

С актом ознакомлен :

\_\_\_\_\_  
(дата)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(расшифровка подписи)

Приложение 7  
к Политике  
информационной безопасности  
администрации Угловского сельского  
поселения Бахчисарайского района  
Республики Крым

**ЖУРНАЛ**  
учета нарушений информационной безопасности,  
ликвидации их причин и последствий  
администрации Угловского сельского поселения Бахчисарайского района  
Республики Крым

Начато «\_\_» \_\_\_\_\_ 20\_\_ г.  
Окончено «\_\_» \_\_\_\_\_ 20\_\_ г.  
Кол-во листов \_\_\_\_\_  
Срок хранения \_\_\_\_\_

Дата	Выявленное нарушение	Должность, фамилия сотрудника, выявившего нарушение	Подпись	Принятые меры Дата, должность, фамилия, Подпись
1	2	3	4	5