АДМИНИСТРАЦИЯ

РАКИТНЕНСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ

Хабаровского муниципального района Хабаровского края

РАСПОРЯЖЕНИЕ

17.02.2023 № 14-р

1Об утверждении правил и процедур в сфере защиты информационных систем, технических средств, персональных данных, идентификации и аутентификации субъектов доступа и объектов доступа, управления доступом субъектов доступа к объектам доступа, регистрации событий безопасности

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», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»:

1. Утвердить прилагаемые:

1.1. Правила и процедуры идентификации и аутентификации субъектов доступа и объектов доступа (приложение № 1).

1.2. Правила и процедуры управления доступом субъектов доступа  
к объектам доступа (приложение № 2).

1.3. Правила и процедуры регистрации событий безопасности (приложение № 3).

1.4. Правила и процедуры антивирусной защиты информационных систем (приложение № 4).

1.5. Правила и процедуры контроля установки обновлений программного обеспечения (приложение № 5).

1.6. Правила и процедуры защиты технических средств (приложение № 6).

1.7. Правила и процедуры обеспечения защиты персональных данных при их передаче по каналам связи, имеющим выход за пределы   
контролируемой зоны (приложение № 7).

2. Контроль за выполнением настоящего распоряжения оставляю за собой.

3. Настоящее распоряжение вступает в силу после его подписания.

Глава сельского поселения С.В. Матвеев

Приложение № 1

к распоряжению администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края

от 17.02.2023 № 14-р \_\_\_\_\_\_\_\_\_\_\_

**Правила и процедуры**

**идентификации и аутентификации субъектов доступа и объектов**

**доступа**

1. Общие сведения

В настоящем разделе рассмотрены:

1. правила и процедуры идентификации и аутентификации пользователей;
2. правила и процедуры управления идентификаторами;
3. правила и процедуры управления средствами аутентификации.

Правила и процедуры идентификации и аутентификации пользователей

Идентификация и аутентификация пользователей в информационных системах, являющихся работниками оператора (далее также – внутренние пользователи, ИС). Идентификация и аутентификация пользователей в ИС при наличии технической возможности должна производиться с использованием служб каталогов (Microsoft Active Directory, Рабочие группы и др.).

Идентификация внутренних пользователей в ИС должна осуществляться по уникальным учетным записям (персональным идентификаторам), однозначно идентифицирующим пользователя.

В качестве идентификаторов внутренних пользователей могут использоваться:

1. имя учетной записи (логин);
2. служебные идентификаторы устройств или служб (наименование,  
   IP-адрес, MAC-адрес, ID-процесса и т.п.);
3. совокупность идентификаторов, указанных выше.

Для каждого персонального идентификатора должна быть определена следующая информация о пользователе: фамилия, имя, отчество пользователя, должность, место работы, рабочий телефон.

Для каждого группового идентификатора по возможности должна быть определена следующая информация о пользователе: наименование отдела, роль пользователя.

Идентификаторы (учетные записи пользователей) объединяются в группы по принципам:

1. пользователи ИС объединяются в группы с ограниченными привилегиями (пользователь, опытный пользователь и т.п.);
2. администраторы ИС объединяются в группы с расширенными привилегиями (например, администратор домена, локальная учетная запись администратора) согласно своим должностным обязанностям.

Учет идентификаторов, выданных внутренним пользователям, может производиться:

1. средствами службы каталогов (для идентификаторов, указанных выше);
2. при передаче устройства идентификации пользователю с оформлением соответствующего акта или путем ведения журнала (Приложение А) (для идентификаторов, указанных выше).

Идентификатор пользователя должен однозначно сопоставляться с запускаемыми от его имени процессами.

Гостевые учетные записи и учетные записи, заданные по умолчанию, в рамках выполнения мер защиты ИС должны быть отключены.

Для аутентификации внутренних пользователей используется пароль;

При использовании пароля в качестве аутентификационной информации допускается сохранение пароля в персональном идентификаторе пользователя. Не допускается сохранение пароля в персональных идентификаторах пользователей, осуществляющих доступ в ИС с правами привилегированных учетных записей.

При использовании в ИС более одного пароля для аутентификации, все пароли должны различаться не менее чем на три символа.

В ИС авторизация пользователей может осуществляться при совершении следующих действий:

1. при входе внутренних пользователей ИС в операционную систему;
2. доступе к средствам администрирования и управления средствами защиты, объектам поддерживающей инфраструктуры, техническим средствам и аппаратным платформам (для средств, в которых предусмотрена отдельная авторизация);
3. начале взаимодействия с прикладным программным обеспечением (только для прикладного программного обеспечения, в котором предусмотрены процессы авторизации пользователей).

Для всех процессов авторизации в ИС действует следующее правило:

1. при предъявлении зарегистрированного в системе идентификатора и при предоставлении верных аутентифицирующих пользователя данных пользователю предоставляется доступ к элементу ИС;
2. при предъявлении неверных идентификатора или данных, аутентифицирующих пользователя, доступ к ресурсам ИС не предоставляется, а пользователю выводится соответствующее сообщение;
3. тип применяемого идентификатора и аутентифицирующих пользователя данных определятся процедурой авторизации пользователя.

Лицо, ответственное за обеспечение информационной безопасности в администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края (далее – администрация) разрабатывает приложение к техническому паспорту ИС (или иной документ) с параметрами авторизации пользователей, определяющий типы идентификаторов и факторы аутентификации, которые в них используются.

2. Правила и процедуры управления идентификаторами

Жизненный цикл идентификаторов и средств аутентификации операционных систем

Создание

Создание идентификатора осуществляется на основании приказа о приеме на работу и (или) назначении на должность лиц, не имевших средств авторизации.

Сведения о возможных типах идентификаторов и средств аутентификации представлены в разделе 1 настоящих Правил и процедур идентификации и аутентификации субъектов доступа и объектов доступа.

В ИС используется два типа учетных записей:

1) постоянные идентификаторы – учетные записи пользователей, работающих с ИС, срок действия идентификатора – до увольнения или перехода работника на должность, не связанную с выполнением работ в ИС;

1. временные идентификаторы – учетные записи, которые создает лицо, ответственное за обеспечение информационной безопасности в администрации, на определенный срок для проведения пусконаладочных, ремонтно-восстановительных, отладочных и иных работ, срок действия идентификатора – не более 90 дней (при необходимости может быть продлен).

Требования к созданию идентификаторов:

1. имя учетной записи в ИС должно быть уникальным;

перед созданием учетной записи лицо, ответственное за обеспечение информационной безопасности в администрации, должно убедиться, что данная учетная запись не используется в ИС;

перед созданием учетной записи лицо, ответственное за обеспечение информационной безопасности в администрации, должно убедиться, что данная учетная запись ранее не использовалась или была удалена более года назад.

Первичный ввод пароля может осуществляться:

1. самостоятельно пользователем при создании учетной записи лицом, ответственным за обеспечение информационной безопасности в администрации;

Лицо, ответственное за обеспечение информационной безопасности в администрации, при этом используется принцип одноразовых паролей (при задании пароля для учетной записи устанавливается параметр «сменить пароль при следующем входе в систему»).

3. Эксплуатация и вывод из эксплуатации

В процессе эксплуатации возможны следующие события, связанные с применением средств идентификации и аутентификации:

1. смена пароля;

2) блокирование учетной записи.

Смена пароля в ИС может быть:

1. плановая – производиться самостоятельно пользователем при истечении максимального срока действия пароля;
2. внеплановая – производиться лицом, ответственным за обеспечение информационной безопасности в администрации, при компрометации пароля или смене забытого пользователем пароля.

Блокирование учетной записи пользователя производится:

1. временное – при превышении числа неверных попыток ввода пароля в ИС. Блокирование осуществляется на определенный период времени, учетная запись может быть разблокирована лицом, ответственным за обеспечение информационной безопасности в администрации;

постоянное – блокирование учетной записи осуществляется лицом, ответственным за обеспечение информационной безопасности в администрации, при компрометации парольной информации или истечения надобности в учетной записи.

Вывод из эксплуатации идентификаторов осуществляется при изменении полномочий пользователя по доступу к средствам вычислительной техники (переход на другую должность, увольнение и т.п.) или истечении срока действия временной учетной записи. Вывод идентификаторов из эксплуатации осуществляется путем удаления учетной записи.

4. Жизненный цикл идентификаторов и средств аутентификации прикладного программного обеспечения (для внутренних и внешних пользователей)

Создание

Создание идентификаторов для внутренних и внешних пользователей осуществляется на основании согласованной с лицом, ответственным за обеспечение информационной безопасности в администрации, служебной записки с указанием обоснования. Под обоснованием понимается приказ о приеме на работу и (или) о назначении на должность лиц, не имевших средств авторизации, а также государственный контракт или договор на оказание услуг.

Сведения о возможных типах идентификаторов и средств аутентификации представлены в разделе 2 настоящего документа.

В ИС используется два типа учетных записей в прикладном программном обеспечении:

1. постоянные идентификаторы – учетные записи пользователей, работающих с ИС, срок действия идентификатора – до увольнения или перехода работника на должность, не связанную с выполнением работ в ИС;
2. временные идентификаторы для внешних пользователей – учетные записи, создающиеся лицом (подразделением), ответственным за управление идентификаторами и аутентификаторами в ИС, на определенный срок для проведения пусконаладочных, ремонтно-восстановительных, отладочных и иных работ, срок действия идентификатора – не более 90 дней (при необходимости может быть продлен).

Требования к созданию идентификаторов идентичны с разделом 2 настоящих правил и процедур.

5. Эксплуатация и вывод из эксплуатации

В процессе эксплуатации возможны следующие события, связанные с применением средств идентификации и аутентификации:

1. смена пароля;
2. блокирование учетной записи.

Смена пароля внешнего пользователя в прикладном программном обеспечении ИС может быть:

1. плановая, производится самостоятельно пользователем при истечении максимального срока действия пароля;
2. внеплановая, производится лицом (подразделением), ответственным за управление идентификаторами и аутентификаторами в ИС, при компрометации пароля или смене забытого пользователем пароля.

Блокирование учетной записи внешнего пользователя бывает:

1. временное, при превышении числа неверных попыток ввода пароля в ИС. Блокирование осуществляется на определенный период времени, учетная запись может быть разблокирована лицом (подразделением), ответственным за управление идентификаторами и аутентификаторами в ИС;
2. постоянное, блокирование учетной записи осуществляется лицом (подразделением), ответственным за управление идентификаторами и аутентификаторами в ИС, при компрометации парольной информации или истечении надобности в учетной записи.

Порядок вывода из эксплуатации идентификаторов осуществляется   
аналогично с разделом 3 настоящих правил и процедур.

6. Правила и процедуры управления средствами аутентификации

В ИС ответственным за хранение, выдачу, инициализацию, блокирование средств аутентификации является лицо, ответственное за обеспечение информационной безопасности в администрации.

На всех средствах вычислительной техники должна быть изменена аутентификационная информация (средств аутентификации), заданная их производителями.

Для ИС устанавливаются и регистрируются следующие характеристики паролей:

1. длина пароля;
2. алфавит пароля (при наличии соответствующих механизмов);
3. максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки программно-технического средства или учетной записи пользователя;
4. время блокировки программно-технического средства или учетной записи пользователя после превышения количества неуспешных попыток аутентификации (ввода неправильного пароля);
5. максимальное время действия пароля;
6. минимальное время действия пароля;
7. минимальное число последних использованных паролей при создании новых паролей.

Сведения о характеристиках паролей, параметрах блокирования учетных записей при превышении количества неуспешных попыток аутентификации приводятся в техническом паспорте ИС.

Средства ввода пароля должны исключать возможность просмотра действительного значения аутентификационной информации за счет скрытого отображения вводимых символов (символы не отображаются либо заменяются на «\*»).

Глава сельского поселения С.В. Матвеев

Приложение А

к Правилам и процедурам идентификации и аутентификации субъектов доступа и объектов доступа

Заявка на создание учетных записей и изменение прав доступа пользователей в

*(наименование информационного ресурса)*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Действие | Ф.И.О. работника (отчество – при наличии) (полностью) | Долж-ность | Подразде-ление | Телефон работника | Права доступа | Дата вступления в силу | Ф.И.О. (отчество – при наличии) и телефон автора заявки |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

В столбце 1 следует указать порядковый номер записи.

В столбце 2 следует указать один из вариантов, например, «создание нового пользователя», «смена пароля», «изменение пользователя», «добавление прав доступа», «удаление прав доступа» или «удаление пользователя», «изменение должности пользователя» и т.д.

В столбце 3 следует указать Ф.И.О. (отчество – при наличии) работника, для которого необходимо создать учетную запись, изменить права доступа или удалить учетную запись.

В столбце 4 следует указать должность работника, для которого необходимо создать учетную запись или изменить права доступа.

В столбце 5 следует указать подразделение работника, для которого необходимо создать учетную запись или изменить права доступа.

В столбце 6 следует указать контактный телефон работника, на которого заводится учетная запись.

В столбце 7 следует указать роль в информационном ресурсе, которую должен иметь работник (допускается пустая графа).

В столбце 8 следует указать дату, с которой вступает в силу создание/изменение прав доступа для данного пользователя.

В столбце 9 следует указать Ф.И.О. (отчество – при наличии) и телефон работника, который оформлял заявку на создание учетной записи или изменение прав пользователя.

Приложение № 2

к распоряжению администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края

от 17.02.2023 № 14-р\_\_\_\_\_\_\_\_\_\_\_

**Правила и процедуры**

**управления доступом субъектов доступа к объектам доступа**

1. Общие сведения

В настоящем разделе рассмотрены:

1) правила и процедуры управления учетными записями пользователей;

2) правила и процедуры блокирования сеансов доступа;

3) правила и процедуры управления информационными потоками;

4) правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации;

5) правила и процедуры применения удаленного доступа;

6) правила и процедуры применения мобильных технических средств.

2. Правила и процедуры управления учетными записями пользователей

Для каждого пользователя информационной системы (далее – ИС) должны быть определены минимально необходимые права доступа, в соответствии с их должностными инструкциями и выполняемыми задачами.

Методы разграничения доступа в ИС определяются лицом, ответственным за обеспечение информационной безопасности в администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края (далее – администрация), фиксируются в технической документации на ИС, которая утверждается руководителем администрации.

Для ИС определяется лицо, ответственное за управление учетными записями (создание, присвоение, уничтожение идентификаторов пользователей и устройств, а также за хранение, выдачу, инициализацию, блокирование средств аутентификации).

Создание новой учетной записи в ИС производится на основании служебной записки после верификации пользователей.

Верификация пользователей, являющихся работниками администрации (внутренние пользователи), при создании учетной записи производится главой администрации.

Верификация пользователей, не являющихся работниками администрации, при создании учетной записи производится лицом, ответственным за управление идентификаторами в пределах делегированной ему области.

Верификация пользователей производится любыми доступными методами и способами (проверка актуальности действия приказа о приеме на работу работника, проверка документов, удостоверяющих личность и др.).

Лицо, ответственное за обеспечение информационной безопасности в администрации, обязано производить пересмотр и при необходимости корректировку учетных записей пользователей ИС в рамках закрепленных за ним областей администрирования, не реже одного раза в 90 дней.

В ИС должен осуществляться пересмотр и при необходимости оповещение лица, ответственного за обеспечение информационной безопасности в администрации поселения, об изменении учетных данных, ролей, обязанностей, полномочий и ограничений пользователей:

1) пересмотр данных внутренних пользователей проводят руководители структурных подразделений;

2) при изменении данных внешних и внутренних пользователей   
оповещается лицо, ответственное за обеспечение информационной безопасности в администрации.

Обязанность оповещения лица, ответственного за обеспечение информационной безопасности в администрации, должна быть закреплена в должностной инструкции начальника отдела кадров администрации (или лица, на которое возложены обязанности по кадровому обеспечению администрации поселения).

В ИС допускается создавать временные учетные записи пользователей по согласованию с лицом, ответственным за обеспечение информационной безопасности в администрации.

Временными учетными записями пользователей являются учетные записи, предоставленные для однократного и/или ограниченного по времени выполнения задач в ИС.

При создании временной учетной записи должно быть обеспечено добавление описания учетной записи с пометкой о принадлежности и времени использования.

Лицо, ответственное за обеспечение информационной безопасности в администрации, обязано производить уничтожение временных учетных записей.

Лицо, ответственное за обеспечение информационной безопасности в администрации, должно вести учет временных учетных записей, заведенных для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования ИС.

Учет временных учетных записей допускается вести в электронном виде. Рекомендуемая форма журнала временных учетных записей представлена в Приложении А к настоящим Правилам и процедурам управления доступом субъектов доступа к объектам доступа.

Доступ к редактированию журнала учета временных учетных записей должен быть ограничен для непривилегированных пользователей.

Лицо, ответственное за обеспечение информационной безопасности в администрации, обязано производить уничтожение (блокирование) неактивных (неиспользуемых) учетных записей после 90 дней неиспользования.

В ИС запрещается использовать гостевые учетные записи пользователей.

Любые привилегированные учетные записи могут создаваться исключительно по согласованию с лицом, ответственным за обеспечение информационной безопасности в администрации.

Создание привилегированных учетных записей осуществляется на основании документально оформленной заявки, согласованной с лицом, ответственное за обеспечение информационной безопасности в администрации. Типовая форма заявки представлена в Приложении Б к настоящим Правилам и процедурам управления доступом субъектов доступа к объектам доступа.

3. Правила и процедуры блокирования сеансов доступа

Лицом, ответственным за обеспечение информационной безопасности в администрации, устанавливаются и регистрируются следующие характеристики блокирования сеансов доступа:

1) максимальное время бездействия, после которого обеспечивается блокирование сеанса доступа пользователя;

2) запрет или разрешение на отображение сведений о пользователе, если сеанс заблокирован;

3) механизмы, с использованием которых будет реализовываться блокирование сеансов доступа;

4) ограничение числа параллельных сеансов доступа.

Установленные для ИС характеристики отображаются в техническом паспорте ИС.

Реализацию установленных для ИС характеристик по блокированию сеансов доступа осуществляет лицо, ответственное за обеспечение информационной безопасности в администрации.

4. Правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации

Перечень действий пользователей до прохождения ими процедур идентификации и аутентификации определяется лицом, ответственное за обеспечение информационной безопасности в администрации.

Установленный для ИС перечень действий, разрешенных до авторизации, приводится в техническом паспорте ИС.

Правила и процедуры управления информационными потоками

В ИС должны обеспечиваться следующие правила управления информационными потоками при передаче информации между устройствами:

1) ИС должна быть сегментирована и отделена от сторонних информационных систем. В ИС сегментирование производится с использованием технологий VLAN или физического разделения;

2) правила управления информационными потоками (правила фильтрации информационных потоков) в ИС должны быть реализованы по принципу «все входящие потоки запрещены»; исходящие разрешены по принципу «разрешено все, что явно не запрещено»;

3) использование сертифицированных средств криптографической защиты информации при ее передаче через сеть Интернет или другие сети связи общего пользования.

Подробная информация о схемах информационных потоков в ИС должна быть представлена в техническом паспорте ИС.

5. Правила и процедуры применения удаленного доступа

Удаленный доступ к ресурсам ИС возможен только с использованием защищенных каналов связи. Защита каналов связи может быть обеспечена:

1) комплексом организационно-технических мер – прокладкой линий связи в пределах контролируемой зоны;

2) применением сертифицированных средств криптографической защиты информации при использовании сетей связи общего пользования, сети Интернет, арендованных каналов связи и т.п.

Лицо, ответственное за обеспечение информационной безопасности в администрации, для ИС устанавливает перечень совместимых средств криптографической защиты информации, с использованием которых может осуществляться доступ к ИС.

Виды удаленного доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) к ИС устанавливаются на этапе ее проектирования, согласуются с лицом, ответственным за обеспечение информационной безопасности в администрации, фиксируются в технической документации на ИС.

Лицом, ответственным за обеспечение информационной безопасности в администрации, определяется перечень совместимых средств криптографической защиты информации, с использованием которых может осуществляться доступ к ИС.

При осуществлении удаленного доступа в ИС пользователи должны проходить процедуры идентификации и аутентификации в соответствии с установленными для ИС правилами и процедурами.

Лицо, ответственное за обеспечение информационной безопасности в администрации, не реже одного раза в месяц осуществляет мониторинг событий удаленного доступа в ИС на предмет выявления несанкционированного удаленного доступа к объектам доступа ИС.

Для ИС должно использоваться ограниченное (минимально необходимое) количество точек подключения при организации удаленного доступа.

Для ИС устанавливается запрет или разрешение удаленного доступа от имени привилегированных учетных записей (администраторов) для администрирования этих систем и их систем защиты информации.

6. Правила и процедуры применения мобильных технических средств

Ответственным за использование мобильных технических средств в ИС является лицо, ответственное за обеспечение информационной безопасности в администрации.

В ИС в качестве мобильных технических средств могут применяться съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (планшеты, сотовые телефоны (за исключением личных сотовых телефонов работников администрации), цифровые камеры, звукозаписывающие устройства и иные устройства).

Для ИС устанавливается возможность использования мобильных технических средств (исходя из технологического процесса обработки информации), что должно быть отражено в технической документации на ИС. Решение по использованию в ИС мобильных технических средств должно быть согласовано с лицо, ответственное за обеспечение информационной безопасности в администрации.

В ИС мобильные технические средства допускается использовать только тем субъектам доступа, для которых использование таких мобильных технических средств необходимо для выполнения своих должностных обязанностей.

Учет портативных вычислительных устройств ведется в журналах учета мобильных технических средств или в специализированном программном обеспечении на основании идентификаторов этих устройств (MAC-адрес, имя устройства и т.д.).

В ИС запрещено использовать не входящие в ее состав (находящиеся в личном использовании) съемные машинные носители информации.

В ИС запрещено использовать съемные машинные носители информации, для которых не определен владелец (пользователь, учреждение, ответственные за принятие мер защиты информации).

Глава сельского поселения С.В. Матвеев

Приложение А

кПравилам и процедурам управления доступом субъектов доступа к объектам доступа

Журнал учета временных учетных записей

(типовая форма)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Наименование временной учетной записи | Ф.И.О. (отчество – при наличии) работника, создавшего временную учетную запись | Цель, для которой создана временная учетная запись | Срок действия временной учетной записи | Ф.И.О. (отчество – при наличии) работника, для которого создана временная учетная запись | Отметка о блокировании (уничтожении) временной учетной записи с указанием даты |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

В столбце 1 следует указать порядковый номер записи.

В столбце 2 следует внести наименование временной учетной записи в соответствии с вновь созданной учетной записью на контроллере домена.

В столбце 3 следует указать Ф.И.О. (отчество – при наличии) работника, создавшего временную учетную запись.

В столбце 4 следует указать цель, для которой создана временная учетная запись.

В столбце 5 следует указать срок действия временной учетной записи.

В столбце 6 следует указать Ф.И.О. (отчество – при наличии) работника, для которого создана временная учетная запись.

В столбце 7 следует внести отметку о блокировании (уничтожении) временной учетной записи с указанием даты.

Приложение Б

кПравилам и процедурам управления доступом субъектов доступа к объектам доступа

Заявка на создание (предоставление) привилегированных прав   
в информационных системах

Должность (кому)

Наименование учреждения

Ф.И.О. (отчество – при наличии) (кому)

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность

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

ФИО (отчество – при наличии)

Служебная записка

В связи с \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*указывается обоснование необходимости делегирования повышенных привилегий*) прошу \_\_\_\_\_\_\_\_\_\_\_\_\_ (*указывается действие: создать учетную запись, изменить привилегии для существующей учетной записи*) \_\_\_\_\_\_\_\_\_\_\_\_ (*указывается Ф.И.О. (отчество – при наличии) субъекта доступа*) для доступа к \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*указывается область делегирования привилегий: наименование ИС/информационного ресурса/сервиса и т.п.*). Срок жизни повышенных привилегий – \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (постоянный, временный (*указывается конкретный срок*)).

Должность Фамилия, инициалы

Дата

Приложение № 3

к распоряжению администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края

от 17.02.2023 № 14-р \_\_\_\_\_\_\_\_\_\_\_

**Правила и процедуры**

**регистрации событий безопасности**

1. Общие сведения

В настоящем разделе рассмотрены:

1) правила и процедуры сбора, записи и хранения информации о событиях безопасности;

2) правила и процедуры реагирования на сбои при регистрации событий безопасности;

3) правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них;

4) правила и процедуры защиты информации о событиях безопасности.

2. Правила и процедуры сбора, записи и хранения информации  
о событиях безопасности

Для информационной системы (далее – ИС) определяется перечень событий безопасности, подлежащих регистрации.

Для ИС перечень регистрируемых событий безопасности приводится в техническом паспорте ИС. Перечень регистрируемых событий безопасности определяется лицом, ответственным за обеспечение информационной безопасности в администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края (далее – администрация), в соответствии со сферами ответственности и наличием технической возможности регистрации событий безопасности.

Для журналов событий каждой технологии/сервиса определяется минимальный срок хранения журналов событий.

Минимально необходимый набор регистрируемых событий безопасности:

Для средств анализа защищенности:

1) служебные события:

а) дата срабатывания события (день, час, минута, секунда);

б) источник события;

в) код события (критическое, предупреждение, ошибка);

2) события безопасности:

а) вход в консоль;

б) выход из консоли;

в) результат попытки входа (успешная или неуспешная).

Для средств межсетевого экранирования:

1) служебные события:

а) дата срабатывания события (день, час, минута, секунда);

б) отправитель события;

в) переполнение свободного пространства в местах хранения логов;

2) события безопасности:

а) дата срабатывания события (день, час, минута, секунда);

б) сетевой интерфейс;

в) IP-адрес источника;

г) IP-адрес назначения;

д) протокол;

е) порт источника;

ж) порт назначения;

з) тип события (блокирован/пропущен);

и) направление;

к) широковещание;

л) количество пакетов;

м) размер;

н) ethernet-протокол.

Для операционных систем:

1) служебные события:

а) дата срабатывания события (день, час, минута, секунда);

б) источник события;

в) пользователь;

г) код события (критическое, предупреждение, ошибка);

2) события безопасности:

а) дата срабатывания события (день, час, минута, секунда);

б) вход в систему;

в) выход из системы;

г) результат попытки входа (успешная или неуспешная);

д) результат попытки загрузки (останова) операционной системы (успешная или неуспешная);

е) идентификатор, предъявленный при попытке доступа;

ж) блокировка учетной записи субъекта доступа.

Для систем антивирусной защиты информации:

1) служебные события:

а) дата срабатывания события (день, час, минута, секунда);

б) запуск задачи (сканирования, обновления и др.);

в) изменение настроек компонентов защиты;

г) результат;

2) события безопасности:

а) дата срабатывания события (день, час, минута, секунда);

б) запуск задачи (сканирования, обновления и др.);

в) изменение настроек компонентов защиты;

г) результат события;

Для прикладного программного обеспечения:

1) служебные события:

а) дата срабатывания события (день, час, минута, секунда);

б) запуск приложения;

в) остановка приложения;

г) изменение настроек приложения;

д) переполнение свободного пространства в местах хранения логов;

2) события безопасности:

а) дата срабатывания события (день, час, минута, секунда);

б) вход в систему;

в) выход из системы;

г) результат попытки входа (успешная или неуспешная);

д) результат попытки загрузки (останова) операционной системы (успешная или неуспешная);

е) идентификатор, предъявленный при попытке доступа;

ж) блокировка учетной записи субъекта доступа.

При отсутствии технической возможности обеспечить регистрацию событий лицом, ответственным за обеспечение информационной безопасности в администрации поселения, осуществляется:

1) анализ влияния отсутствия регистрации определенных событий безопасности на обеспечение защиты информации в ИС;

2) принятие решения о необходимости реализации компенсирующих мер;

3) разработка комплекса компенсирующих мер, снижающих негативное влияние, отсутствие регистрации определенных событий безопасности (при необходимости).

3. Правила и процедуры реагирования на сбои при регистрации событий безопасности

При обнаружении сбоев лицо, ответственное за обеспечение информационной безопасности в администрации, и (или) администратор ИС:

1) проводит их устранение в течение двух рабочих дней;

2) инициирует служебную проверку по факту сбоев.

Время оповещения руководителя администрации о сбоях в работе – в течение 8 часов с момента обнаружения сбоя.

4. Правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них

Лицо, ответственное за обеспечение информационной безопасности в администрации, или уполномоченные работники не реже одного раза в месяц осуществляют мониторинг событий безопасности всего перечня событий безопасности, подлежащих регистрации в ИС.

Лицо, ответственное за обеспечение информационной безопасности в администрации, не реже одного раза в месяц осуществляет мониторинг событий безопасности всего перечня событий безопасности, подлежащих регистрации на АРМ пользователей, в составе не менее 25% от общего состава, входящего в состав ИС.

Лицом, ответственным за обеспечение информационной безопасности в администрации, и уполномоченными работниками осуществляется еженедельный оперативный мониторинг критичных событий безопасности ИС на предмет выявления критичных событий безопасности информации. В число критичных источников для мониторинга включаются:

1) средства антивирусной защиты информации;

2) средства обнаружения и предотвращения вторжений;

3) средства защиты информации от несанкционированного доступа (в части событий, сигнализирующих о признаках несанкционированного доступа).

Дополнительно к событиям, перечисленным выше, лицом, ответственным за обеспечение информационной безопасности в администрации, могут быть определены дополнительные категории событий безопасности, требующие еженедельного оперативного мониторинга.

При выявлении признаков инцидентов безопасности в ИС:

1) проводятся мероприятия по реагированию на выявленные инциденты безопасности в течение двух рабочих дней;

2) осуществляется планирование проведения подобных мероприятий.

По запросу лица, ответственного за обеспечение информационной безопасности в администрации, результаты мониторинга оформляются в виде отчета.

5. Правила и процедуры защиты информации о событиях безопасности

В ИС необходимо осуществлять сбор, запись и хранение информации о событиях безопасности в течение времени, установленного лицом, ответственным за обеспечение информационной безопасности в администрации.

Сбор, запись и хранение информации о событиях безопасности должны предусматривать:

1) возможность выбора лицом, ответственным за обеспечение информационной безопасности в администрации, событий безопасности, подлежащих регистрации в текущий момент времени, из перечня событий безопасности;

2) генерацию записей регистрации для событий безопасности, подлежащих регистрации;

3) хранение информации о событиях безопасности в течение времени, установленного лицом, ответственным за обеспечение информационной безопасности в администрации.

Защита информации о событиях безопасности обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с настоящими Правилами и процедурами регистрации событий безопасности, и, в том числе, включает защиту средств ведения регистрации и настроек механизмов регистрации событий, а также путем резервирования журналов событий.

В ИС необходимо обеспечить резервное копирование записей регистрации (аудита).

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

Контроль реализации методов защиты журналируемой информации в ИС осуществляет лицо, ответственное за обеспечение информационной безопасности в администрации поселения, не реже одного раза в год.

Логическое ограничение доступа к местам хранения журналов событий.

Ограничение физического доступа посторонних в помещения, где размещены технические средства, в которых хранятся журналы событий.

Предоставление права управления журналами событий, просмотр результатов журналов регистрации событий только пользователям, обладающим правами доступа в соответствии с разрешительной системой доступа.

Реализация правил разграничения доступа к журналам регистрации событий и (или) средствам управления механизмами регистрации событий осуществляется в соответствии с Правилами и процедурами управления доступом.

Глава сельского поселения С.В. Матвеев

Приложение № 4

к распоряжению администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края

от 17.02.2023 № 14-р \_\_\_\_\_\_\_\_\_\_\_

**Правила и процедуры**

**антивирусной защиты информационных систем**

1. Общие сведения

В настоящем разделе рассмотрены:

1) правила и процедуры антивирусной защиты информационных систем (далее – ИС);

2) правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов).

2. Правила и процедуры антивирусной защиты ИС

Средства антивирусной защиты (далее – САЗ) применяются:

1) на автоматизированных рабочих местах (далее – АРМ) ИС;

2) в периметральных средствах защиты информации (средствах межсетевого экранирования и других средствах защиты информации), где существует техническая возможность;

3) иных точках доступа в ИС.

Установка, конфигурирование и управление САЗ осуществляется лицом, ответственным за обеспечение информационной безопасности в администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края (далее – администрация).

В ИС должны применяться только лицензионные и сертифицированные ФСТЭК России САЗ.

В рамках централизованной системы антивирусной защиты установка, конфигурирование и управление САЗ осуществляются администраторами ИС совместно с лицом, ответственным за обеспечение информационной безопасности в администрации.

Параметры настройки САЗ, используемых в ИС, определяются лицом, ответственным за обеспечение информационной безопасности в администрации, в соответствии с требованиями по защите информации, предъявляемыми к ИС.

Доступ к консоли управления ограничивается паролем с учетом требований парольной защиты в администрации.

Пользователям запрещается отключать САЗ и самостоятельно вносить изменения в их настройки.

Лицо, ответственное за обеспечение информационной безопасности в администрации, производит установку парольного доступа к настройкам САЗ.

При подключении внешних и съемных носителей информации в ИС проводится автоматическая проверка на наличие вирусных программ.

Мониторинг событий САЗ и реагирование на вирусное заражение осуществляется лицом, ответственным за обеспечение информационной безопасности в администрации. Мониторинг событий САЗ в ИС и реагирование на вирусное заражение осуществляется администраторами ИС. Мониторинг САЗ осуществляется оперативно в рабочее время. Периодичность мониторинга – ежедневно.

Лицо, ответственное за обеспечение информационной безопасности в администрации при необходимости формирует отчет о вирусной активности.

В случае обнаружения вредоносных программ пользователи ИС обязаны:

1) приостановить все операции, связанные с обработкой информации на АРМ;

2) немедленно сообщить о факте заражения:

а) лицу, ответственному за обеспечение информационной безопасности в администрации поселения;

б) источнику получения файла (его владельцам) при достоверно установленном владельце.

Возобновить работу на АРМ только после удаления вирусной программы и нейтрализации последствий вирусного заражения.

Лицо, ответственное за обеспечение информационной безопасности в администрации выполняет следующие действия:

1) принимает меры по удалению вирусной программы (лечению) и нейтрализации последствий вирусного заражения;

2) при невозможности удаления (лечения) принимает меры по нейтрализации возможности деструктивного воздействия со стороны вирусной программы;

3) при необходимости инициирует проведение служебного расследования по факту вирусного заражения.

3. Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов)

Обновление сигнатур осуществляется в автоматическом режиме по заданному расписанию.

Источником обновлений являются:

1) серверы обновлений производителей САЗ;

2) иные источники, предоставляемые федеральными органами исполнительной власти, уполномоченными в области безопасности информации.

Минимальная периодичность проверки и получения обновлений – один раз в неделю.

Глава сельского поселения С.В. Матвеев

Приложение № 5

к распоряжению администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края

от 17.02.2023 № 14-р \_\_\_\_\_\_\_\_\_\_\_

**Правила и процедуры**

**контроля установки обновлений программного обеспечения**

На всех элементах информационных систем (далее – ИС) (при технической возможности) должен быть обеспечен запрет установки обновлений средств защиты информации (далее – СрЗИ) от имени непривилегированных пользователей.

Сертифицированные по требованиям безопасности информации СрЗИ должны обновляться с доверенных источников обновлений сертифицированной поддержки продуктов.

Запрещается устанавливать настройки обновлений СрЗИ с общедоступных недоверенных источников обновлений.

Доверенным источником обновлений считается:

1) источник обновлений, который указан в паспорте-формуляре средств защиты информации;

2) источник обновлений, который установлен по умолчанию при установке СрЗИ с сертифицированного дистрибутива продукта.

Установка обновлений несертифицированных операционных систем, используемых в ИС, при наличии технической возможности должна проводиться в автоматическом режиме с серверов разработчиков операционных систем или развернутых серверов обновлений.

При отсутствии технической возможности автоматической установки обновлений несертифицированных операционных систем, используемых ИС, установка осуществляется в ручном режиме.

Установка обновлений прикладного и системного программного обеспечения, используемого в ИС, проводится лицом, ответственным за обеспечение информационной безопасности в администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края.

Данные об установке обновлений прикладного программного обеспечения должны быть зафиксированы в технической документации на ИС. Допускается фиксация установки обновлений средствами прикладного, системного или специализированного программного обеспечения.

Глава сельского поселения С.В. Матвеев

Приложение № 6

к распоряжению администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края

от 17.02.2023 № 14-р\_\_\_\_\_\_\_\_\_\_\_

**Правила и процедуры**

**защиты технических средств**

1. Общие сведения

В настоящем разделе рассмотрены правила и процедуры контроля и управления физическим доступом.

2. Правила и процедуры контроля и управления физическим доступом

Для информационных систем (далее – ИС) определяется перечень лиц, имеющих право доступа в помещения, в которых установлены технические средства ИС.

Данный перечень утверждается главой Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края (далее - поселение).

Способами физической защиты рабочих кабинетов могут быть:

1) надежно запираемые металлические замки;

2) обеспечение физической охраны на договорной основе;

3) охранная сигнализация;

4) установка системы контроля и управления доступом;

5) видеонаблюдение;

6) совокупность вышеуказанных мер.

При использовании средств опечатывания необходимо вести журналирование открытия/закрытия помещения(ий) (Приложение А).

Проведение ремонтных, наладочных или других работ в рабочих кабинетах допускается только в присутствии работников, имеющих право самостоятельного доступа в них.

Устройства вывода изображения технических средств (мониторы) должны быть размещены таким образом, чтобы обеспечить невозможность случайного ознакомления с посетителей или иных лиц, не допущенных к обработке защищаемой информации (не допускается ориентация монитора на окно, дверной проем и т.п.).

Режим безопасности организуют и обеспечивают работники администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края (далее – администрация).

Контроль за организацией режима безопасности в помещениях, в которых расположены технические средства ИС, осуществляет лицо, ответственное за обеспечение информационной безопасности в администрации.

Нахождение лиц в помещениях ИС, не включенных в перечень лиц, имеющих право доступа в эти помещения, возможно только в сопровождении лица, ответственного за обеспечение информационной безопасности в администрации или другого должностного лица на время, необходимое для решения вопросов, связанных с осуществлением полномочий в рамках договоренности, заключенной с оператором ИС.

Доступ в помещения, в которых осуществляется обработка защищаемой информации, в нерабочее время возможен только по письменной заявке.

Факты санкционированного физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, лиц, не допущенных в данные помещения, фиксируются лицом, ответственным за обеспечение информационной безопасности в администрации в соответствующем журнале (Приложение Б).

При возникновении нештатных ситуаций (пожар, затопление):

1) производится локализация источника опасности своими силами, если это не угрожает жизни и здоровью людей;

2) оповещается лицо, ответственное за обеспечение информационной безопасности в администрации, а также глава поселения или лицо, его заменяющее, о возникновении нештатной ситуации с целью получения указаний по защите информации при данной ситуации.

В случае если действия, указанные выше, противоречат действиям, указанным в инструкциях по охране труда и технике безопасности, последние имеют более высокий приоритет.

При возникновении нештатных ситуаций допускается вскрытие помещений, в которых осуществляется обработка защищаемой информации с целью сведения к минимуму негативных последствий нештатной ситуации (негативных последствий).

При вскрытии помещения, в котором осуществляется обработка защищаемой информации, составляется акт, а также инициируется служебное расследование по поводу причин возникновения нештатной ситуаций с целью предотвращения ее повторного возникновения.

Глава сельского поселения С.В. Матвеев

Приложение А

к Правилами процедурам защиты технических средств

Журнал

опечатывания (опломбирования) (наименование рабочего кабинета, серверного помещения)  
(типовая форма)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Дата и время закрытия | № печати (пломбы) | Ф.И.О. (отчество – при наличии) лица, закрывшего помещение | Подпись лица, закрывшего кабинет/помещение | Дата и время вскрытия кабинета/помещения | Отметка о соответствии номера печати (пломбы), подпись лица, вскрывшего кабинет/помещение |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Настоящий журнал разрабатывается для каждого помещения, в котором обрабатывается защищаемая  
 информация (персональные данные).

Приложение Б

к Правилам и процедурам защиты технических средств

Журнал

учета физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены  
(типовая форма)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование объекта доступа/расположение | Ф.И.О. (отчество – при наличии) лица, допущенного к объекту доступа | Дата и время получения доступа | Цель получения доступа |
|
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

В столбце 1 следует указать порядковый номер записи.

В столбце 2 следует указать наименование объекта доступа (к чему осуществляется доступ).

В столбце 3 следует указать фамилию, имя, отчество (последнее – при наличии) лица, допущенного к объекту доступа. Для лиц, не являющихся сотрудниками администрации поселения, следует указать должность и наименование учреждения, которое это лицо представляет.

В столбце 4 следует указать дату и время получения доступа.

В столбце 5 следует указать цель получения доступа к объекту доступа.

Приложение № 7

к распоряжению администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края

от 17.02.2023 № 14-р\_\_\_\_\_\_\_\_\_\_\_

**Правила и процедуры**

**обеспечения защиты персональных данных при их передаче по каналам связи, имеющим выход за пределы контролируемой зоны**.

Запрещается передача персональных данных в явном виде по открытым каналам связи, имеющим выход за пределы контролируемой зоны.

При необходимости передачи персональных данных по каналам связи, имеющим выход за пределы контролируемой зоны сотрудник администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края обязан уведомить лицо, ответственное за обеспечение информационной безопасности в администрации Ракитненского сельского поселения Хабаровского муниципального района Хабаровского края. Для защиты от раскрытия, модификации и навязывания передача информации такого рода должна осуществляться исключительно по защищенным каналам связи.

Глава сельского поселения С.В. Матвеев