Приложение к постановлению
Администрации Улуг-Хемского кожууна
от «__» _____ 2020г №____

ПОЛИТИКА
информационной безопасности
в администрации Улуг-Хемского кожууна

г. Шагонар
2020

I. Назначение

1.1. В соответствии с:

- п.2), п.4), п.6) ч.1 и ч.2 ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ст.2 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, утвержденного Постановлением Правительства Российской Федерации от 21.03.2012 №211;
- п.2.12, п.4.1, п.4.3 ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий;
- п.3.1.48, п. А.6.3 ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;
- разд.5.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п.3.2.4 и разд. 3.6 ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология и др.

в организациях должен быть разработан документ под названием Политика информационной безопасности (Правила информационной безопасности), который определяет общую совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

1.2. Целью Политики информационной безопасности в администрации Улуг-Хемского кожууна (далее - Политики) является определение основных правил обеспечения безопасности объектов защиты администрации Улуг-Хемского кожууна от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, а также минимизации ущерба от возможной реализации угроз безопасности защищаемой информации.

1.3. Структура Политики разработана в соответствии с Примерным перечнем вопросов, входящих в состав политики безопасности информационных технологий организации.

1.4. В соответствии с:

- ч.2. ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ст.2 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, утвержденного Постановлением Правительства РФ от 21.03.2012 №211;
- п. 5.1.3 ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий,

Администрация Улуг-Хемского кожууна обязана опубликовать, разместить на официальном сайте или иным образом обеспечить неограниченный доступ к настоящей Политике.

II. Область применения

1.1. Настоящая Политика определяет общие правила, процедуры, практические приемы и руководящие принципы в области безопасности информации, которыми руководствуется администрация Улуг-Хемского кожууна в своей деятельности. В Политике определены объекты защиты, общий замысел защиты информации администрации Улуг-Хемского кожууна, требования к пользователям информационных систем, степень ответственности сотрудников, структура и необходимый уровень защищенности, статус и должностные обязанности лиц, ответственных за обеспечение безопасности информации, обрабатываемой в информационных системах администрации Улуг-Хемского кожууна.

1.2. Требования Политики обязательны для всех работников администрации Улуг-Хемского кожууна, представителей контрольно-надзорных органов, допущенных к защищаемой информации на законных основаниях, а также индивидуальных лиц и работников иных организаций, допущенных к защищаемой информации для проведения работ по государственным контрактам или иным гражданско-правовым договорам.

III. Термины, обозначения и сокращения

2.1. В настоящей Политике используются следующие термины и обозначения:

2.1.1. **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.

2.1.2. **Администратор безопасности информации** - лицо, отвечающее за защиту информационных систем от несанкционированного доступа к информации, за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации.

2.1.3. **Аутентификация -** проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе)[1].

2.1.4. **Безопасность информации [данных]** - 1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность[2]; 2) состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами[3].

2.1.5. **Виртуализация** - технология преобразование формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

2.1.6. **Идентификация** - присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

2.1.7. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.1.8. **Информационные системы администрации Улуг-Хемского кожууна** – информационные системы, включая информационные системы персональных данных, представляющие собой совокупность информации, содержащейся в базах данных, и обеспечивающих ее обработку информационных технологий и технических средств.

2.1.9. **Инцидент** - непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или

---

[1] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[2] См.:

- п. 2.4.5 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения;
- п.3.1.4 «Рекомендации по стандартизации Р.50.1.053 – 2005. Информационная технология. Основные термины и определения в области защиты информации».

[3] См. п. 1.6. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 №282.

возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

2.1.10. **Контролируемая зона** – это пространство, в котором исключено неконтролируемое пребывание работников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

2.1.11. **Машинные носители информации** - физическое устройство (дискета, e-Token, смарт-карта и т.д.), предназначенное для хранения информации в электронной форме.

2.1.12. **Межсетевой экран (средство межсетевого экранирования)** - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС[4].

2.1.13. **Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или информационными системами.

2.1.14. **Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

2.1.15. **Объект защиты информации** - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

2.1.16. **Оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

2.1.17. **Оператор персональных данных (оператор ПДн)** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.1.18. **Ответственный за организацию обработки персональных данных** – главный специалист отдела правового, кадрового

---

[4] См.:

- п.1.19. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- раздел 3 Руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утвержденные решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25.07.1997.

обеспечения и по наградам администрации Улуг-Хемского кожууна, осуществляющее:

- внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения сотрудников администрации Улуг-Хемского кожууна положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организацию прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляющее контроль за приемом и обработкой таких обращений и запросов.

2.1.19. **Политика безопасности (информации в организации)** - совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

2.1.20. **Регуляторы** - Федеральная служба по техническому и экспортному контролю (ФСТЭК России)[5], Федеральная служба безопасности (ФСБ России)[6], Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)[7].

2.2. В настоящем Положении используются следующие сокращения:

2.2.1. **АС**- автоматизированная система;

2.2.2. **ИС**- информационная система;

---

[5] Полномочия установлены в соответствии с:

- ч.9 ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ч.5 ст.16 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации";
- ст.1 Положения о Федеральной службе по техническому и экспертному контролю, утвержденному Указом Президента Российской Федерации от 16.08.2004 №1085.

[6] Полномочия установлены в соответствии с:

- ч.9 ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ст.11.2, п. «и.1» ст.12 Федерального закона от 03.04.1995 №40-ФЗ "О Федеральной службе безопасности";
- ст.5 Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденного Постановлением Правительства РФ от 16.04.2012 №313.

[7] Полномочия установлены в соответствии с:

- ст.23 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ст.1. и ст.5 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного Постановлением Правительства РФ от 16.03.2009 №228.

2.2.3. **ИСПДн**- информационная система персональных данных;
2.2.4. **КЗ** - контролируемая зона;
2.2.5. **КСЗИ**- криптографическое средство защиты информации;
2.2.6. **МНИ**- машинные носители информации;
2.2.7. **МЭ** - межсетевой экран;
2.2.8. **НСД**- несанкционированный доступ;
2.2.9. **Оргмеры** - организационные меры защиты персональных данных;
2.2.10. **ПДн**- персональные данные;
2.2.11. **СЗИ**- средства защиты информации;
2.2.12. **СЭД**- система электронного документооборота;
2.2.13. **УЧРЕЖДЕНИЕ** – Администрация Улуг-Хемского кожууна.

IV. Объекты и общий замысел защиты информации администрации Улуг-Хемского кожууна

4.1. Объектами защиты администрации Улуг-Хемского кожууна являются:
4.1.1. информационные ресурсы, содержащие конфиденциальную информацию, а также открытая (общедоступная) информация, необходимая для работы администрации Улуг-Хемского кожууна, независимо от формы и вида ее представления;
4.1.2. процессы обработки информации в информационных системах администрации Улуг-Хемского кожууна, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;
4.1.3. информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены элементы информационной среды.
4.2. Общий замысел защиты информации исходит из того, что:

- безопасность защищаемой информации достигается путем исключения несанкционированного, в том числе случайного, доступа к защищаемой конфиденциальной информации (включая и персональные данные), результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий;
- выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и осуществления конкретных мероприятий по обеспечению безопасности конфиденциальной информации (включая и персональные данные) в администрации Улуг-Хемского кожууна;

- информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей;
- должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных;
- должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

4.3. Основополагающим принципом построения системы защиты информации информационных систем администрации Улуг-Хемского кожууна является следующее положение: в соответствии с положениями нормативных правовых актов Регуляторов и внутренних распорядительных актов в администрации Улуг-Хемского кожууна применяются требования для защиты информации, содержащейся в государственных информационных системах.

V. Организация и инфраструктура информационной безопасности в администрации Улуг-Хемского кожууна

5.1. Организация информационной безопасности в администрации Улуг-Хемского кожууна

Организация информационной безопасности в администрации Улуг-Хемского кожууна заключается в:

- определении лиц, ответственных за организацию и поддержание информационной безопасности в администрации Улуг-Хемского кожууна;
- регламентации оборота конфиденциальной информации на бумажных и электронных носителях;
- обучении пользователей по вопросам информационной безопасности.

5.1.1. Лица, ответственные за организацию и поддержание информационной безопасности в администрации Улуг-Хемского кожууна

5.1.1.1. Председатель администрации Улуг-Хемского кожууна как первый руководитель Учреждения несет персональную ответственность за регламентацию порядка безопасной обработки конфиденциальной информации и обеспечение требований по защите конфиденциальной информации.

5.1.1.2. Специалист по информационным системам несет ответственность за защиту информационных систем от несанкционированного доступа к информации, за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации информационных систем.

5.1.1.3. Специалист по информационным системам и главный специалист по информатизации и связи несут ответственность за поддержание

уровня защищенности информационных систем администрации Улуг-Хемского кожууна

5.1.1.4. Лицо, ответственное за организацию обработки персональных данных, несет ответственность за:

- осуществление внутреннего контроля за соблюдением работниками законодательства Российской Федерации о защите персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников администрации Улуг-Хемского кожууна положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организации приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществлении контроля за приемом и обработкой таких обращений и запросов;
- осуществление контроля организации допуска работников администрации Улуг-Хемского кожууна к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

5.1.2. Обучение пользователей по вопросам информационной безопасности

5.1.2.1. Перед допуском к самостоятельной работе с информацией ограниченного доступа пользователи должны быть соответствующим образом проинструктированы начальником отдела информационных технологий (или уполномоченным лицом, на который возложены обязанности по защите информации) или иным образом обучены правилам обращения с конфиденциальной информацией и средствами защиты информации.

5.2 Инфраструктура информационной безопасности в администрации Улуг-Хемского кожууна

Инфраструктура информационной безопасности заключается в:

- определении ролей и обязанностей должностных лиц по обеспечению информационной безопасности;
- регулярной проверке согласованности мер защиты информации;
- обработке инцидентов, связанных с нарушением безопасности.

5.2.1. Определение ролей и обязанностей должностных лиц по обеспечению информационной безопасности

5.2.1.1. Определены следующие категории лиц, допущенных к работе в информационных системах администрации Улуг-Хемского кожууна:

- администратор информационной системы;
- пользователь.

5.2.1.2. Данные о группах пользователей и администраторов, уровне их доступа и информированности отражены также в Положении о разрешительной системе допуска пользователей к информационным системам администрации Улуг-Хемского кожууна.

5.2.1.3. Администратор информационной системы:

5.2.1.3.1. Администратор информационной системы – должностное лицо администрации Улуг-Хемского кожууна или уполномоченное лицо (работник уполномоченного лица)[8], ответственное за настройку, внедрение и сопровождение информационных систем. Администратор информационной системы обеспечивает функционирование подсистемы управления доступом ИС и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя к элементам, хранящим защищаемую информацию.

5.2.1.3.2. Администратор информационной системы обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИС;
- обладает полной информацией о технических средствах и конфигурации ИС;
- имеет доступ ко всем техническим средствам обработки информации и данным ИС;
- обладает правами конфигурирования и административной настройки технических средств ИС.

5.2.1.4. Пользователь:

5.2.1.4.1. Пользователь - должностное лицо администрации Улуг-Хемского кожууна или иного государственного (муниципального) органа (организации), допущенный в установленном порядке к работе с защищаемой информацией, полномочия которого регламентированы внутренними нормативно-правовыми актами администрации Улуг-Хемского кожууна. Обработка защищаемой информации включает: возможность просмотра информации, ручной ввод информации в информационную систему, формирование справок и отчетов по информации, полученной из ИС. Пользователь не имеет полномочий для управления подсистемами обработки данных.

5.2.1.4.2. Пользователь обладает следующим уровнем доступа и знаний:

[8] Осуществляющее свои функциональные обязанности по гражданско-правовому договору, заключенному в соответствии с ч.3 ст.6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации;
- располагает конфиденциальными данными, к которым имеет доступ.

5.2.2. Обработка инцидентов, связанных с нарушением безопасности информации

5.2.2.1. В администрации Улуг-Хемского кожууна должны проводиться следующие мероприятия по обработке инцидентов, связанных с нарушением безопасности информации:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;
- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий[9];
- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

VI. Безопасность аппаратно-программного обеспечения в администрации Улуг-Хемского кожууна

Безопасность аппаратно-программного обеспечения в администрации Улуг-Хемского кожууна должна достигаться проведением следующих мероприятий:

- идентификацией и аутентификацией субъектов доступа;

- управлением доступом субъектов доступа к объектам доступа;
- мониторингом (просмотром, анализом) результатов регистрации событий безопасности и реагирование на них;
- уничтожением (стиранием) данных и остаточной информации с машинных носителей информации и (или) уничтожением машинных носителей информации;
- антивирусной защитой;
- обеспечением безопасности персональных компьютеров;
- обеспечением безопасности среды виртуализации;
- регламентацией и контролем в информационной системе мобильных технических средств;
- установкой (инсталляцией) только разрешенного к использованию программного обеспечения и (или) его компонентов.

6.1. Управление доступом субъектов доступа к объектам доступа

6.1.1. Меры по управлению доступом субъектов доступа к объектам доступа в информационные системы администрации Улуг-Хемского кожууна должны обеспечиваться управлением правами и привилегиями субъектов доступа, разграничением доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечении контроля соблюдения этих правил[10].

6.1.2. При управлении доступом субъектов доступа к объектам доступа в информационные системы администрации Улуг-Хемского кожууна должны проводиться следующие мероприятия:

6.1.2.1. реализуемое администратором безопасности информации при помощи средств управления СЗИ управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

6.1.2.2. реализация путем создания защищенных каналов связи средствами ПАК «ViPNet Coordinator HW1000» защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно телекоммуникационные сети;

6.1.2.3. регламентация и контроль использования в информационной системе технологий беспроводного доступа, заключающихся в

[10] Исполняется в соответствии с:

- п. 20.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.2.3, п.3.2, п. методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

применении одинакового набора средств защиты информации для всех узлов независимо от каналов связи;

6.1.2.4. регламентация и контроль использования в информационной системе мобильных технических средств, заключающихся в применении одинакового набора средств защиты информации для всех узлов независимо от каналов связи;

6.1.2.5. управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы);

6.1.2.6. обеспечение доверенной загрузки средств вычислительной техники.

6.2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации

6.2.1. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации в администрации Улуг-Хемского кожууна должно производиться при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

6.2.2. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, в установленном порядке должно осуществляться физическое уничтожение этих машинных носителей информации.

6.3. Антивирусная защита в информационных системах администрации Улуг-Хемского кожууна

6.3.1. Безопасность аппаратно-программного обеспечения в администрации Улуг-Хемского кожууна от разрушающего воздействия компьютерных вирусов достигается также проведением мероприятий по антивирусной защите, основанных на следующих принципах:

6.3.1.1. Контроль состояния антивирусной защиты ИС администрации Улуг-Хемского кожууна возлагается на специалиста по информационным системам или уполномоченное лицо.

6.3.1.2. К использованию в ИС допускаются только сертифицированные антивирусные средства, централизованно закупленные у разработчиков (или официальных поставщиков) указанных средств.

6.3.1.3. В администрации Улуг-Хемского кожууна ежедневно в начале работы при загрузке компьютеров в автоматическом режиме обязан проводиться автоматический контроль всех дисков и файлов.

6.3.1.4. Должно обеспечиваться автоматическое централизованное обновление вирусных сигнатур и антивирусного ПО на всех ПЭВМ, работающих в ИС.

6.3.1.5. Обязательному автоматическому антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных (несъемных) носителях (магнитных дисках, CD-ROM, флэш и т.п.).

6.3.1.6. Разархивирование и контроль входящей информации обязан проводиться непосредственно после ее приема на выделенном автономном компьютере или на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающей аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный машинный носитель информации).

6.3.1.7. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

6.3.1.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

6.4. Обеспечение безопасности персональных компьютеров администрации Улуг-Хемского кожууна

6.4.1. Безопасность персональных компьютеров в администрации Улуг-Хемского кожууна должна достигаться осуществлением мер физического и логического контроля доступа.

6.4.2. Меры физического контроля доступа к средствам вычислительной техники (физическая защита) регламентируются нормативными правовыми актами Регуляторов и внутренними организационно - распорядительными актами.

6.4.3. Политика в отношении логического доступа к компьютерам заключается в:

- установлении правил разграничения доступа и контроля соблюдения этих правил;
- контроле доступа пользователей к средствам вычислительной техники информационной системы с целью предотвращения неавторизованного доступа к информационным системам (контроле регистрации пользователей, управлении привилегиями доступа, контроле в отношении паролей пользователей, пересмотре прав доступа пользователей и др.).

6.5. Обеспечение безопасности среды виртуализации[11]

[11] В настоящее время в администрации Улуг-Хемского кожууна среда виртуализации не применяется. В настоящей Политике излагаются общие принципы построения системы защиты среды виртуализации в случае ее применения.

6.5.1. Для обеспечения безопасности виртуальной среды должны применяться меры защиты аналогичные применяемым в физической среде, но с учетом специфических особенностей виртуальной среды, а именно[12]:

- идентификация и аутентификация субъектов доступа как внутри виртуальной среды, так и при доступе к средствам управления виртуальной инфраструктурой;
- управления доступом субъектов доступа к объектам доступа внутри виртуальной среды и при доступе к средствам управления этой средой;
- управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры;
- регистрация событий безопасности в виртуальной инфраструктуре;
- управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;
- контроль целостности виртуальной инфраструктуры и ее конфигураций;
- резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры;
- реализация и управление антивирусной защитой в виртуальной инфраструктуре;
- разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.
-

VII. Телекоммуникационная безопасность администрации Улуг-Хемского кожууна

С целью защиты как внутренних, так и внешних сетевых сервисов в администрации Улуг-Хемского кожууна должны осуществляться контроль сетевого доступа, для обеспечения которого при необходимости определяются:

[12] Исполняется в соответствии с:

- п. ЗСВ.1 – п. ЗСВ.4, п. ЗСВ.6- п. ЗСВ.10 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.2.3, разд.3.11 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);

- политика в отношении использования сетевых служб;
- предопределенный маршрут;
- аутентификация пользователей в случае внешних соединений;
- принципы разделения в сетях;
- контроль сетевых соединений;
- управление маршрутизацией сети;
- безопасность использования сетевых служб;
- политика в отношении электронной почты.

7.1. Политика в отношении использования сетевых служб

7.1.1. В администрации Улуг-Хемского кожууна установлен разрешительный режим доступа к сетевым службам[13].

7.1.2. В связи с тем, что несанкционированные подключения к сетевым службам могут нарушать информационную безопасность администрации Улуг-Хемского кожууна, пользователям должен обеспечиваться непосредственный доступ только к тем сервисам, в которых они были авторизованы.

7.1.3. В целях контроля сетевого доступа должны определяться:

- сети и сетевые услуги, к которым разрешен доступ;
- процедуры авторизации для определения кому, к каким сетям и сетевым сервисам разрешен доступ;
- мероприятия и процедуры по защите от несанкционированного подключения к сетевым сервисам.

7.2. Аутентификация узлов в случае внешних соединений

7.2.1. Аутентификация узлов в случае внешних соединений в администрации Улуг-Хемского кожууна должна достигаться средствами криптографии.

7.3. Принцип разделения в сетях

7.3.1. В администрации Улуг-Хемского кожууна по управлению информационной безопасностью в пределах сети должны разделяться группы информационных сервисов, пользователей и информационные системы.

7.3.2. Критерии для разделения сетей на домены формируются на основе анализа политики контроля доступа, а также учитывая влияние этого разделения на производительность в результате включения подходящей технологии маршрутизации сетей или шлюзов.

---

[13] См.:

- п. 5.4.2 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282.

7.4. Контроль сетевых соединений

7.4.1. В администрации Улуг-Хемского кожууна для контроля сетевого доступа должны применяться мероприятия по управлению информационной безопасностью, чтобы ограничивать возможности пользователей по подсоединению. Такие мероприятия могут быть реализованы посредством сетевых шлюзов, которые фильтруют трафик с помощью определенных таблиц или правил. Применяемые ограничения должны основываться на политике и требованиях доступа к бизнес-приложениям, а также соответствующим образом поддерживаться и обновляться.

7.4.2. Ограничения должны применяться к следующим бизнес-приложениям:

- электронная почта;
- передача файлов в одном направлении;
- передача файла в обоих направлениях;
- интерактивный доступ;
- доступ к сети, ограниченный определенным временем суток или датой.

7.5. Управление маршрутизацией сети

7.5.1. В администрации Улуг-Хемского кожууна для обеспечения информационной безопасности при осуществлении маршрутизации должен осуществляться контроль адресов источника и назначения сообщения. Преобразование сетевых адресов осуществляется для изоляции сетей и предотвращения распространения маршрутов от сети одного подразделения администрации Улуг-Хемского кожууна в сеть другого.

7.6. Безопасность использования сетевых служб

7.6.1. Безопасность использования сетевых служб в администрации Улуг-Хемского кожууна должна достигаться использованием только сертифицированных средств защиты информации, централизованно закупленных у разработчиков (или официальных поставщиков) указанных средств.

7.7. Политика в отношении электронной почты

7.7.1. В администрации Улуг-Хемского кожууна для обеспечения информационной безопасности должны быть регламентированы

правила использования электронной почты, предусматривающие следующие аспекты:

- вероятность атаки на электронную почту (вирусы, перехват);
- защиту вложений в сообщения электронной почты;
- данные, при передаче которых не следует пользоваться электронной почтой;
- исключение возможности компрометации администрации Улуг-Хемского кожууна со стороны сотрудников, например, путем рассылки дискредитирующих и оскорбительных сообщений, использование корпоративной электронной почты с целью неавторизованных покупок;
- использование криптографических методов для защиты конфиденциальности и целостности электронных сообщений;
- хранение сообщений, которые, в этом случае, могли бы быть использованы в случае судебных разбирательств;
- дополнительные меры контроля обмена сообщениями, которые не могут быть аутентифицированы.

VIII. Физическая безопасность в администрации Улуг-Хемского кожууна

8.1. Физическая безопасность в администрации Улуг-Хемского кожууна должна достигаться проведением мероприятий, касающихся как внешних[14], так и внутренних[15] аспектов.

8.2. Физическая безопасность от внешних угроз должна достигаться:

- установлением контролируемой зоны;
- контролем доступа посторонних лиц в помещения контролируемой зоны в рабочее и нерабочее время.

8.3. Физическая безопасность от внутренних угроз должна достигаться:

- прочностью строительных конструкций здания;
- противопожарной защитой и пожарной сигнализацией;
- регламентацией действий персонала при возгорании, предотвращении и (или) минимизации ущерба при затоплении водой/жидкостью, отключении электроэнергии;
- защитой коммуникаций и систем обеспечения энергоносителями в зданиях;
- размещением оборудования, исключающим несанкционированный доступ к нему и несанкционированный доступ к видовой информации.

---

[14] Например, окружающей обстановки вокруг здания, возможности проникновения через крышки люков.

[15] Например, прочности конструкции здания, замков, системы пожарной сигнализации и защиты, системы сигнализации при затоплении водой/жидкостью, отказов в энергоснабжении и т.д.

IX. Безопасность персонала администрации Улуг-Хемского кожууна

Вопросы безопасности, связанные с персоналом, заключаются в:

- учете вопросов безопасности при найме персонала;
- включении вопросов информационной безопасности в должностные обязанности;
- соглашении о конфиденциальности;
- условиях трудового договора;
- обучении пользователей;
- реагировании на инциденты нарушения информационной безопасности и сбои.

9.1. Включение вопросов информационной безопасности в должностные обязанности

9.1.1. Функции (роли) и ответственность в области информационной безопасности следует документировать. В должностные обязанности работников администрации Улуг-Хемского кожууна должны включаться как общие обязанности по внедрению или соблюдению политики безопасности, так и специфические особенности по защите определенных активов или действий, касающихся безопасности.

9.2. Соглашение о конфиденциальности

9.2.1. В администрации Улуг-Хемского кожууна регламентирован порядок доступа работников администрации Улуг-Хемского кожууна и сотрудников иных органов и организаций к конфиденциальной информации. Соглашение о конфиденциальности заключается в форме Обязательства работника о неразглашении конфиденциальной информации администрации Улуг-Хемского кожууна и Соглашения о неразглашении конфиденциальной информации администрации Улуг-Хемского кожууна заключаемого с сотрудниками иных органов и организаций, допускаемых к конфиденциальной информации на основании государственных контрактов или гражданско-правовых договоров.

9.2.2. В государственные контракты и гражданско-правовые договоры, заключаемые администрацией Улуг-Хемского кожууна с подрядчиками, которым для выполнения условий контракта (договора) необходим доступ к служебной информации, в соответствии с нормами действующего законодательства включаются положения о соблюдении конфиденциальности.

9.3. Условия трудового договора

9.3.1. В администрации Улуг-Хемского кожууна в соответствии с действующим законодательством устанавливаются условия трудового договора[16], определяющего ответственность работника в отношении информационной безопасности. Указанная ответственность должна сохраняться и в течение 36 месяцев после увольнения со службы. До работника доводятся меры ответственности, которые будут применимы в случае нарушения требований безопасности.

9.4. Обучение пользователей

9.4.1. Обучение пользователей должно проводиться с целью обеспечения уверенности в осведомленности пользователей об угрозах и проблемах, связанных с информационной безопасностью, и их оснащенности всем необходимым для соблюдения требований политики информационной безопасности при выполнении должностных обязанностей.

9.5. Реагирование на инциденты нарушения информационной безопасности и сбои

Реагирование на инциденты нарушения информационной безопасности и сбои осуществляется с целью сведения к минимуму ущерба от инцидентов нарушения информационной безопасности и сбоев и должно заключаться в:

- информировании об инцидентах нарушения информационной безопасности;
- информировании о проблемах безопасности;
- информировании о сбоях программного обеспечения;
- извлечении уроков из инцидентов нарушения информационной безопасности;
- процессе установления дисциплинарной ответственности.

9.5.1. Информирование об инцидентах нарушения информационной безопасности

9.5.1.1. В администрации Улуг-Хемского кожууна должны предусматриваться формализованные процедуры информирования об инцидентах, а также процедуры реагирования на инциденты, устанавливающие действия, которые должны быть предприняты после получения сообщения об инциденте. Все пользователи должны быть ознакомлены с процедурой информирования об инцидентах нарушения информационной безопасности, а также

[16] В соответствии с ч.4 ст.57 Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ.

проинформированы о необходимости незамедлительного сообщения об инцидентах.

9.5.1.2. В администрации Улуг-Хемского кожууна предусматриваются процедуры обратной связи по результатам реагирования на инциденты нарушения информационной безопасности.

9.5.1.3. Информация об инцидентах может использоваться с целью повышения осведомленности пользователей, поскольку позволяет демонстрировать на конкретных примерах возможные последствия инцидентов, реагирование на них, а также способы их исключения в будущем.

9.5.2. Информирование о проблемах безопасности

9.5.2.1. В обязанностях пользователей информационных сервисов предусматривается, что они должны:

- обращать внимание и сообщать о любых замеченных или предполагаемых недостатках и угрозах в области безопасности в системах или сервисах;
- немедленно сообщать об этих причинах для принятия решений своему руководству или непосредственно поставщику услуг.

9.5.2.2. Требования информационной безопасности предусматривают, что пользователи не должны ни при каких обстоятельствах самостоятельно искать подтверждения подозреваемому недостатку в системе безопасности. Это требование предъявляется в интересах самих пользователей, поскольку тестирование слабых мест защиты может быть интерпретировано как неправомочное использование системы.

9.5.3. Информирование о сбоях программного обеспечения

9.5.3.1. Для информирования о сбоях программного обеспечения в администрации Улуг-Хемского кожууна регламентированы соответствующие процедуры, при которых должны предусматриваться следующие действия:

- симптомы проблемы и любые сообщения, появляющиеся на экране, должны фиксироваться;
- по возможности, компьютер необходимо изолировать и пользование им прекратить;
- о факте сбоя программного обеспечения немедленно должен извещаться администратор информационных систем.

9.5.3.2. Пользователи не должны пытаться самостоятельно удалить подозрительное программное обеспечение, если они не уполномочены

на это. Ликвидировать последствия сбоев должен соответственно обученный персонал.

9.5.4. Процесс установления дисциплинарной ответственности

9.5.4.1. По каждому выявленному факту нарушения информационной безопасности в администрации Улуг-Хемского кожууна регламентировано проведение служебной проверки и привлечение виновных к ответственности.

X. Безопасность документов и носителей информации администрации Улуг-Хемского кожууна

10.1. В администрации Улуг-Хемского кожууна в целях информационной безопасности регламентирован полный цикл обращения конфиденциальных документов, в том числе и на электронных носителях (создание или получение, регистрация, пересылка, исполнение, хранение, уничтожение).

10.2. Контроль за оборотом (учетом, выдачей, использованием, передачей, хранением и уничтожением) машинных носителей информации должен осуществляться работниками отдела информационной безопасности.

XI. Обеспечение непрерывности деятельности администрации Улуг-Хемского кожууна, включая планирование действий при чрезвычайных ситуациях и восстановлении после аварий

11.1. В администрации Улуг-Хемского кожууна должно обеспечиваться управление непрерывностью деятельности с целью минимизации отрицательных последствий, вызванных бедствиями и нарушениями безопасности (которые могут быть результатом природных бедствий, несчастных случаев, отказов оборудования и преднамеренных действий), до приемлемого уровня с помощью комбинирования профилактических и восстановительных мероприятий по управлению информационной безопасностью. Проведение указанных мероприятий регламентировано внутренними организационно - распорядительными актами.

11.2. В случае чрезвычайных ситуаций, инцидентов информационной безопасности, способных повлиять на непрерывность информационных процессов администрации Улуг-Хемского кожууна, создается оперативный штаб и рабочая группа оперативного штаба.

11.3. Оперативный штаб возглавляет главный врач председатель администрации Улуг-Хемского кожууна. Место сбора оперативного штаба – зал заседаний администрации Улуг-Хемского кожууна.

11.4. В состав оперативного штаба входят руководители структурных подразделений администрации Улуг-Хемского кожууна.

11.5. В состав рабочей группы оперативного штаба входят специалист по информационным системам, а также иные должностные лица.

11.6. Задача оперативного штаба: активация Плана обеспечения непрерывности и восстановления управления информационных систем администрации Улуг-Хемского кожууна, организация кризисного управления, проведение разбора недостатков кризисного управления после ликвидации ЧП, закрытия инцидента информационной безопасности.

11.7. Задача рабочей группы оперативного штаба: документирование решений оперативного штаба при кризисном управлении, проведение мероприятий кризисного управления, проведение анализа по результатам кризисного управления, подготовка материалов для заседаний оперативного штаба, в том числе и по подведению итогов кризисного управления.

XII. Политика аутсорсинга в администрации Улуг-Хемского кожууна

12.1. В соответствии с требованиями действующего администрация Улуг-Хемского кожууна вправе поручить на договорной основе уполномоченным лицам исполнять следующие функции обеспечения безопасности:

- физическая защита (охрана помещений, пропускной режим, обслуживание охранно-пожарной сигнализации);
- администрирование информационных систем;
- администрирование информационной безопасности и др.

12.2. Лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению администрации Улуг-Хемского кожууна и (или) предоставляющее администрации Улуг-Хемского кожууна вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (уполномоченное лицо), обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации. В договоре должна быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии требованиями по защите информации и настоящей Политикой.

XIII. Ответственность и полномочия

13.1. Ответственность персонала

13.1.1. За нарушение требований настоящей Политики должностные лица администрации Улуг-Хемского кожууна несут

ответственность в соответствии с действующим законодательством.

13.1.2. Должностные лица администрации Улуг-Хемского кожууна, вносящие изменения в конфигурацию информационных систем, несут ответственность за соответствие своих действий процедурам, регламентированным настоящей Политикой.

13.2. Полномочия персонала

13.2.1. Работники администрации Улуг-Хемского кожууна имеют право выходить с предложениями к руководству администрации Улуг-Хемского кожууна по вопросам защиты конфиденциальной информации. Изменения в настоящую Политику вносятся постановлением администрации Улуг-Хемского кожууна после обязательного согласования вносимых изменений со специалистом по информационным технологиям, отвечающим за соответствие вносимых изменений требованиям законодательства и нормативно-правовых актов Регуляторов.