Приложение № 1
к постановлению Администрации
Таштыпского района
29.12.2012 г. № 572

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Область применения

Настоящая Политика информационной безопасности (далее – Политика) в **Администрации Таштыпского района Республики Хакасия** (далее – Администрация) является документом, закрепляющим основные цели, задачи и принципы организации системы обеспечения информационной безопасности.

Документ описывает цели и задачи информационной безопасности, определяет совокупность правил, требований и принципов работы в области информационной безопасности, которыми руководствуется Администрация в своей деятельности.

Требования настоящего документа обязательны для выполнения всеми сотрудниками Администрации.

Политика разработана в соответствии с действующим законодательством в области обеспечения безопасности информации и обеспечения безопасности персональных данных.

2. Нормативные ссылки

В настоящем Положении использованы ссылки на следующие локальные нормативные акты:

- Положение о физической безопасности - Часть 1 - Защита помещений;
- Положение о физической безопасности - Часть 2 - Безопасность оборудования;
- Положение об организации обеспечения информационной безопасности;
- Положение о комиссии по вопросам информационной безопасности;
- Положение об обеспечении информационной безопасности сотрудниками;
- Положение об инцидентах в системе информационной безопасности;
- Положение о персональных данных;
- Положение о классификации и управлении активами;
- Положение об управлении компьютерами и сетями - Часть 1 - Процедуры эксплуатации и распределения ответственности;
- Положение об управлении компьютерами и сетями - Часть 2 - Планирование реализации и приемки систем;
- Положение об управлении компьютерами и сетями - Часть 3 - Защита от вредоносного программного обеспечения;
- Положение об управлении компьютерами и сетями - Часть 4 - Резервное копирование;
- Положение об управлении компьютерами и сетями - Часть 5 - Управление защитой сети;
- Положение об управлении компьютерами и сетями - Часть 6 - Обращение с носителями информации;

- Положение об управлении компьютерами и сетями - Часть 7 - Обмен информацией;
- Положение об управлении компьютерами и сетями - Часть 8 - Осуществление контроля;
- Положение о контроле доступа;
- Положение об эксплуатации и обслуживании информационных систем;
- Положение о соответствии требованиям;
- Положение об организации и обеспечении функционирования шифровальных (криптографических) средств.

3. Термины и определения

В настоящем Положении применены следующие термины с соответствующими определениями:

- **актив** – что-либо, что имеет ценность для Администрации;
- **анализ риска** – систематическое использование информации для выявления источников и для оценки степени риска;
- **доступность** – обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости;
- **защита информации** – сохранение конфиденциальности, целостности и доступности информации; кроме того, также могут быть включены другие свойства, такие как аутентичность, подотчетность, неотрекаемость и надежность;
- **конфиденциальность** – обеспечение доступа к информации только авторизованным пользователям;
- **оценка риска** – целостный процесс анализа риска и оценки значительности риска;
- **риск** – комбинация вероятности события и его последствий;
- **средства обработки информации** – любая система, служба или инфраструктура обработки информации, или фактическое месторасположение, где они находятся;
- **средство управления** – средства управления рисками, включая политику, процедуры, руководящие принципы, практики или организационные структуры, которые могут носить административный, технический, управленческий или юридический характер;
- **третья сторона –** лицо или организация, которые признаются независимыми от вовлеченных сторон в том, что касается рассматриваемой проблемы;
- **угроза –** возможная причина нежелательного инцидента, который может закончиться ущербом для системы или организации;
- **целостность** – обеспечение достоверности и полноты информации и методов ее обработки.

4. Общие положения

Настоящая Политика разработана с целью:

- информирования сотрудников Администрации об осуществляемой деятельности в сфере обеспечения информационной безопасности;
- формирования основ соответствия деятельности Администрации действующему законодательству в области обеспечения информационной безопасности, в том числе персональных данных;

- защиты интересов при обеспечении должного уровня безопасности активов Администрации.

Положения и требования Политики распространяются на всю деятельность Администрации, основных разработчиков и исполнителей, которые участвуют в разработке, создании, развертывании, вводе в эксплуатацию информационной системы, в части, их касающейся.

Положения и требования Политики могут быть распространены (по согласованию) также на другие предприятия, учреждения и организации, осуществляющие информационное взаимодействие в качестве поставщиков и потребителей (пользователей) информации.

Под информационной безопасностью информационной системы понимается состояние защищенности информационной среды (информации, информационных ресурсов, фондов и информационных систем, баз данных), при которой её формирование, использование, развитие и информационный обмен обеспечивается защитой информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования.

Политика является методологической основой для:

1. разработки подсистемы информационной безопасности при доступе к информации, реализуемой на объектах информатизации с ограниченным доступом, в виде комплексной системы защиты информации от несанкционированного доступа;
2. разработки защищенного электронного документооборота, с использованием средств криптографической защиты информации, развертывания системы удостоверяющих центров, применения электронной цифровой подписи и частных виртуальных сетей обмена защищаемой информации;
3. разработки конкретных нормативных документов и мероприятий, регламентирующих деятельность в области обеспечения информационной безопасности;
4. реализации прав граждан, Администрации на получение, распространение и использование информации.

5. Цели политики информационной безопасности

Основными целями политики информационной безопасности является:

1. Понимание и обработка стратегических и оперативных рисков для информационной безопасности, приемлемых для Администрации.
2. Защита конфиденциальности информации о субъектах персональных данных.
3. Сохранение целостности материалов бухгалтерского учета.
4. Соответствие общих веб-сервисов и внутренних сетей соответствующим стандартам и требованиям.

6. Принципы информационной безопасности

Система информационной безопасности строится на базе использования следующих основных принципов:

1. Администрация способствует принятию рисков и преодолевает риски, которые не возможно преодолеть при консервативном управлении, при условии понимания, мониторинга и обработки рисков для информации при необходимости.

2. Все сотрудники Администрации в обязательном порядке информируется о требованиях информационной безопасности и ответственен за информационную безопасность в отношении своих должностных обязанностей.
3. Учреждение принимает необходимые меры для финансирования средств управления информационной безопасностью и процессов управления проектами.
4. Возможности мошенничества и злоупотреблений в области информационных систем принимается в расчет при общем управлении информационными системами.
5. Отчеты о состоянии информационной безопасности являются доступными.
6. Администрация отслеживает риски для информационной безопасности и предпринимает действия, когда изменения приводят к возникновению непредвиденных рисков.
7. Ситуации, которые могут привести к нарушению законов и установленных норм, не должны допускаться.

7. Анализ политики информационной безопасности

Политика информационной безопасности анализируется через запланированные промежутки времени или в случае возникновения значительных изменений, с целью обеспечить ее продолжающееся соответствие, адекватность и результативность.

Анализ политики информационной безопасности включает в себя оценивание возможностей для улучшения организационной политики в области защиты информации и подход к управлению защитой информации в ответ на изменения в организационном окружении, деловых обстоятельствах, юридических условиях или в технической среде.

Анализ политики в области защиты учитывает результаты анализа со стороны руководства. Определяются процедуры анализа со стороны руководства, включая график или период анализа.

Входные данные для анализа со стороны руководства должны включать информацию по следующим вопросам:

1. обратная реакция заинтересованных сторон;
2. результаты независимых анализов, в соответствии с Положением об организации обеспечения информационной безопасности;
3. статус предупреждающих и корректирующих действий, в соответствии с Положением об организации обеспечения информационной безопасности;
4. результаты предыдущего анализа со стороны руководства;
5. выполнение процессов и соответствие политике в области защиты информации;
6. изменения, которые могут повлиять на подход Администрации к управлению защитой информации, включая изменения в организационном окружении, деловых обстоятельствах, доступности ресурсов, договорных, нормативных и юридических условиях или в технической среде;
7. тенденции, связанные с угрозами и слабыми местами;
8. полномочные инциденты в системе защиты информации;
9. рекомендации, предоставленные соответствующими органами.

Выходные данные для анализа со стороны руководства включают любые решения и действия, касающиеся следующего:

1. улучшение подхода организации к управлению защитой информации и ее процессами;
2. улучшение целей и средств управления;
3. улучшение в распределении ресурсов и/или обязанностей.

8. Документы, дополняющие политику информационной безопасности

Система управления информационной безопасностью включает:

- настоящую Политику;
- Положение о физической безопасности - Часть 1 - Защита помещений;
- Положение о физической безопасности - Часть 2 - Безопасность оборудования;
- Положение об организации обеспечения информационной безопасности;
- Положение о комиссии по вопросам информационной безопасности;
- Положение об обеспечении информационной безопасности сотрудниками;
- Положение об инцидентах в системе информационной безопасности;
- Положение о персональных данных;
- Положение о классификации и управлении активами;
- Положение об управлении компьютерами и сетями - Часть 1 - Процедуры эксплуатации и распределения ответственности;
- Положение об управлении компьютерами и сетями - Часть 2 - Планирование реализации и приемки систем;
- Положение об управлении компьютерами и сетями - Часть 3 - Защита от вредоносного программного обеспечения;
- Положение об управлении компьютерами и сетями - Часть 4 - Резервное копирование;
- Положение об управлении компьютерами и сетями - Часть 5 - Управление защитой сети;
- Положение об управлении компьютерами и сетями - Часть 6 - Обращение с носителями информации;
- Положение об управлении компьютерами и сетями - Часть 7 - Обмен информацией;
- Положение об управлении компьютерами и сетями - Часть 8 - Осуществление контроля;
- Положение о контроле доступа;
- Положение об эксплуатации и обслуживании информационных систем;
- Положение о соответствии требованиям;
- Положение об организации и обеспечении функционирования шифровальных (криптографических) средств.

Управляющий делами И.С.Кайлачаков