|  |  |
| --- | --- |
|  | Приложение 6 к приказу комитета по культуре города Барнаула  от 29 июля 2021г. №64 |

ПОЛИТИКА

информационной безопасности

1. Общие положения

1.1.Политика информационной безопасности (далее – Политика) определят основные цели, задачи, общие принципы и направления обеспечения информационной безопасности, внутренних информационных систем и ресурсов комитета по культуре города Барнаула (далее – комитет).

1.2. Под политикой информационной безопасности понимается совокупность управленческих решений, направленных на совершенствование правового и организационного обеспечения информационной безопасности.

1.3. Общим принципом политики информационной безопасности комитета является запрет всех действий и всех видов доступа, которые не разрешены явно данной политикой или документами, определяющими ее реализацию.

1.4. Правовую основу политики информационной безопасности составляют законодательные и нормативные акты Российской Федерации.

2. Цели и задачи

2.1.Основными целями Политики являются:

обеспечение целостности и доступности информации, циркулирующей в сети передачи данных комитета;

защита от незаконного вмешательства в процесс функционирования комитета;

экономически рациональная и эффективная эксплуатации информационных систем и ресурсов;

предотвращение утечки персональных данных информации комитета;

защита от несанкционированного доступа к сетевым и информационным ресурсам комитета;

повышение дисциплинарного уровня сотрудников комитета при работе с внутренними информационными системами и ресурсами.

2.2. Основными задачами обеспечения информационной безопасности сети передачи данных в целом и внутренних ресурсов комитета являются:

обеспечение своевременности и достоверности передачи информации;

прогнозирование и выявление внутренних и внешних угроз информационной безопасности;

защита от несанкционированного вмешательства в процесс функционирования сетей и систем;

защита данных, хранимых и передаваемых по каналам связи от несанкционированной ознакомления, модификации, фальсификации и уничтожения;

защита программных средств от несанкционированной модификации и уничтожения;

контроль целостности операционной среды исполнения прикладных программ (решения прикладных задач) и программных средств, их восстановление в случае нарушения;

защита от утечки информации ограниченного распространения, хранимой, обрабатываемой и передаваемой по каналам связи;

разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам;

регистрация действий пользователей при работе с защищаемыми ресурсами и услугами сетей в системных журналах и периодический контроль корректности действий пользователей системы путем анализа этих журналов;

физическая защита объектов, оборудования, производственных и служебных помещений.

3. Область действия и реализация политики

3.1. Требования Политики распространяются на всех сотрудников комитета.

3.2. Ответственность за реализацию и соблюдение требований политики информационной безопасности возлагается на председателя комитета;

3.3. Контроль за реализацией, а также координацию работ по пересмотру и дополнению Основных положений политики информационной безопасности возлагается на председателя комитета.

3.4. Актуализация политики информационной безопасности производится в обязательном порядке в следующих случаях:

при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности;

при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб комитету;

при изменении политики Российской Федерации в области информационной безопасности, указов и законов Российской Федерации в области защиты информации.

3.5. Основные требования политики информационной безопасности применяются ко всем деловым партнерам и клиентам комитета.

3.6. Комитет несет ответственность за целостность и доступность информации субъектов ИСПДн расположенных на АС и серверах НСПД, а также при ее передаче по НСПД.

4. Угрозы информационной безопасности

4.1. Под информационной безопасностью понимается защищенности информационной среды от существующих и вероятных внешних и внутренних угроз информационным ресурсам.

4.2. Информационными ресурсами являются:

технические средства автоматизации - компьютерное оборудование и средства связи;

прикладное и системное программное обеспечение;

электронные носители информации всех видов;

информация в виде файлов и баз данных на электронных носителях;

бумажные носители;

знания персонала.

4.3. Угроза информационной безопасности - это любое событие, которое потенциально может нанести вред путем раскрытия, модификации или разрушения информации, или отказа в обслуживании критическими сервисами. Угрозы могут быть неумышленными, такими как те, что вызываются ошибками человека, сбоями оборудования или программ, или стихийными бедствиями.

4.4. Типичными угрозами являются:

сбой в работе одной из компонент сети – сбой из-за ошибок при проектировании, ошибок оборудования или программ может привести к отказу в обслуживании или компрометации безопасности из-за неправильного функционирования одной из компонент сети;

сканирование информации - несанкционированный просмотр критической информации злоумышленниками или авторизованными пользователями;

использование оборудования и информации не по назначению – использование оборудования и информации для целей, отличных от авторизованных, может привести к отказу в обслуживании, излишним затратам, потере репутации. Виновниками этого могут быть как внутренние, так и внешние пользователи;

несанкционированное удаление, модификация или раскрытие информации – умышленное искажение информационных ценностей, которое может привести к потере целостности или утечке информации;

атаки неавторизованных субъектов или систем следствием которых являются отказы в обслуживании или значительные затраты на восстановление.

5. Классификация данных

5.1. Все информационные ресурсы подразделяются на соответствующие классы безопасности, каждый из которых должен иметь свои требования по обеспечению безопасности:

5.2. Критическая информация – информация, требующая специальных мер безопасности для обеспечения гарантий ее целостности и защиты от неавторизованной модификации или удаления. Это - информация, которая требует более высоких гарантий, чем обычно в отношении ее точности и полноты (например, информация о финансовых операциях комитета, пароли).