ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО "РЕГИОНАЛЬНЫЙ РАСЧЕТНО-КАССОВЫЙ ЦЕНТР"

Белгород 2010 г.

1 Термины и определения

РРКЦ - АО "Региональный расчетно-кассовый центр"

Поставщик – Организация, предоставляющая населению жилищные, коммунальные и прочие услуги.

2 Цели

Информация — это ресурс, который, как и прочие ресурсы, имеет ценность для РРКЦ и, следовательно, нуждается в должной защите.

Главной целью Политики информационной безопасности АО " Региональный расчетно-кассовый центр" (далее – Политика) является заявление о приверженности РРКЦ к управлению информационной безопасностью для:

- предотвращения мошенничества и финансовых потерь РРКЦ и Поставщиков;
- защиты критичной информации РРКЦ и Поставщиков от несанкционированного доступа;
- обеспечения корректной и бесперебойной работы информационных систем РРКЦ.

Данная Политика устанавливает основополагающие принципы защиты информации в РРКЦ.

За исполнение требований данной Политики генеральный директор РРКЦ несет персональную ответственность.

3 Направления и принципы деятельности

Основополагающими принципами при разработке Политики являются принцип контролируемых полномочий доступа к информации и принцип доверия. Полномочия пользователя (группы пользователей) должны соответствовать степени доверия, которой этот пользователь (группа пользователей) обладает. При этом должны соблюдаться следующие принципы:

- Пользователи заинтересованы в том, чтобы выполнять свои обязанности без избыточного контроля.
- Технический персонал заинтересован в простоте конфигурирования и управления системами обеспечения информационной безопасности.

Отдельными документами регламентируются следующие вопросы:

- Политика категорирования информации и разграничения доступа.
- Политика пользования вычислительными и прочими ресурсами РРКЦ.
- Политика доступа в Интернет, пользования электронной почтой и другими средствами коммуникации (в т.ч. факсимильной связью).
- Политика удаленного доступа (в т.ч. через VPN и беспроводные сети).
- Политика защиты периметра (сетевой защиты).
- Политика антивирусной защиты и противодействия вирусным атакам.
- Парольная политика.
- Вопросы криптографической защиты информации.
- План обеспечения непрерывности деятельности (в т.ч. политика резервного копирования, политика обработки инцидентов информационной безопасности и т.п.).
- Другие аспекты деятельности, связанные с информационными рисками.

4 Требования бизнеса

При разработке Политики и процедур по управлению информационной безопасностью принимается во внимание принцип разумной достаточности, который заключается в том, что расходы на управление информационной безопасностью должны быть пропорциональны размеру вероятного ущерба, наносимого РРКЦ и Поставщикам в результате нарушений информационной безопасности.

5 Требования законодательства

Управление информационной безопасностью в РРКЦ осуществляется в соответствии с действующей законодательной и нормативной базой РФ, в т.ч. Федеральными законами «Об

информации, информационных технологиях и о защите информации», «О коммерческой тайне», «О персональных данных» и др.

6 Требования договоров

Любая информация, принадлежащая или передаваемая третьим сторонам, передается в соответствии с заключенными соглашениями/договорами, содержащими положения о неразглашении.

Разделы договоров, определяющие правила применения средств защиты информации, а также порядок разрешения споров с использованием этих средств, должны соответствовать реально осуществляемой деятельности, применяемым организационным и техническим средствам информационной безопасности.

7 Источники информации

Главным источником информации при определении требований к информационной безопасности является оценка рисков, принимающая во внимание общую бизнес-стратегию и цели РРКЦ. Посредством оценки рисков определяются угрозы в отношении ресурсов, оцениваются уязвимости и вероятность угроз, а также величина возможного ущерба.

В качестве основной методологии при оценке рисков используется оценка вероятности наступления риска и возможных последствий. Критерием принятия риска является решение Генерального директора РРКЦ.

8 Управление персоналом

Политика доводится до сведения всех сотрудников РРКЦ за неделю до утверждения Генеральным директором. Заинтересованные лица имеют возможность внести в Политику согласованные изменения.

Вновь принимаемые на работу сотрудники знакомятся с Политикой до подписания трудового договора.

9 Последствия нарушения политики информационной безопасности

За нарушения требований Политики и иных подчинённых ей документов виновные несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством РФ.

10 Пересмотр политики информационной безопасности

Политика должна пересматриваться через запланированные интервалы времени или в случае, если произошли существенные изменения деятельности, для того чтобы обеспечить ее пригодность, адекватность и эффективность.