KM Life®
KELESHEK MURASY

Выдержка из политики информационной безопасности АО «КСЖ «KM Life»

ЦЕЛИ, ЗАДАЧИ, ТРЕБОВАНИЯ И ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

Целью Политики информационной безопасности АО «КСЖ «KM Life» (далее – Компания) является обеспечение конфиденциальности, целостности и доступности информации для снижения рисков и экономических потерь, связанных со всевозможными угрозами, присущими информационным ресурсам Компании, а также предотвращение утечки конфиденциальной информации и недопущение несанкционированного доступа. С этой целью поддерживаются вышеуказанные свойства информации, а именно:

1) конфиденциальность - свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;

2) целостность - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);

3) доступность - свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия.

Построение системы обеспечения информационной безопасности (далее – ИБ) Компании и ее функционирование осуществляются в соответствии со следующими основными принципами:

1) законность - любые действия, предпринимаемые для обеспечения ИБ, осуществляются на основе действующего законодательства с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Компании;

2) ориентированность на бизнес - ИБ рассматривается как процесс поддержки основной деятельности Компании. Любые меры по обеспечению ИБ не должны повлечь за собой серьезных препятствий деятельности Компании;

3) непрерывность - применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Компании осуществляются без прерывания или остановки текущих бизнес-процессов Компании;

4) комплексность - обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла на всех технологических этапах их использования во всех режимах функционирования;

5) обоснованность и экономическая целесообразность - используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем ИБ должна быть меньше размера возможного ущерба от любых видов риска;

6) приоритетность - категорирование (ранжирование) всех информационных ресурсов Компании по степени важности при оценке реальных, а также потенциальных угроз ИБ;

7) необходимое знание и наименьший уровень привилегий - пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

8) специализация - эксплуатация технических средств и реализация мер ИБ должны осуществляться профессионально подготовленными специалистами Компании;

9) информированность и персональная ответственность - руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях ИБ и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер ИБ;

10) взаимодействие и координация - меры ИБ осуществляются на основе взаимосвязи Службы безопасности со структурными подразделениями Общества, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

11) подтверждаемость - важная документация и все записи - документы, подтверждающие исполнение требований по ИБ и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

Основными объектами (активами) обеспечения ИБ являются следующие элементы:

1) информационные ресурсы, содержащие сведения ограниченного распространения и представленные в виде документов или записей в носителях на магнитной, оптической и другой основе, информационных физических полях, массивах и базах данных;

2) программные средства (системы управления базами данных, СПО и ППО) ИС, с помощью которых производится обработка информации;

3) автоматизированные системы связи и передачи данных (средства телекоммуникации);

4) каналы связи, по которым передается информация;

5) средства вычислительной техники, предназначенные для обработки, хранения и передачи электронных информационных ресурсов (аппаратные средства).

Согласовано:

Специалист по информационной безопасности	_____	Е. Боранбаев
Начальник Отдела технического сопровождения	_____	У. Копанов
Начальник Службы комплаенс	_____	А.Кембаева
Начальник Управления по правовому обеспечению	_____	Е. Доронина