ООО «Управляющая Компания «Тикет Хаус»»

УТВЕРЖДАЮ
Генеральный директор
«УК «Тикет Хаус»»
_____ **Д.Л.Горин**
"9" октября 2017 г.

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

ПОЛИТИКА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Москва
2017 г.

1. ВВЕДЕНИЕ

1.1. Одним из важнейших активов Общества является информация, значимая для его деятельности, в том числе полученная в ходе взаимодействия со сторонними организациями и физическими лицами.

2.2. Нарушение требований ИБ может привести к серьезным последствиям, таким как финансовые потери, правовые санкции, ущерб репутации Общества, в том числе потеря доверия со стороны клиентов и партнеров, снижение конкурентоспособности Общества.

3.3. Надлежащий уровень ИБ в Обществе достигается в соответствии с требованиями бизнеса путем внедрения СУИБ и совершенствования обеспечивающих ИБ процессов, основываясь на принципах международных стандартов и практик.

2. ОБЛАСТЬ ДЕЯТЕЛЬНОСТИ СУИБ

2.1. СУИБ распространяется на все бизнес-процессы Общества, так как важно обеспечить их безопасность и непрерывность для стабильного функционирования деятельности Общества.

3. ЦЕЛИ И ЗАДАЧИ СУИБ

3.1. Основная цель внедрения СУИБ – создание и постоянное поддержание в Обществе условий, при которых риски, связанные с обеспечением безопасности активов Общества, постоянно контролируются и находятся на приемлемом уровне.

3.2. Достижение данной цели позволяет:

- защитить активы Общества от всех видов угроз (внешних и внутренних, умышленных и непреднамеренных);

- обеспечить непрерывность бизнеса;

- минимизировать ущерб, наносимый бизнесу в результате возникновения инцидентов ИБ;

- увеличить прибыли на инвестированный капитал и получить дополнительные возможности для бизнеса.

3.3. Вышеописанная цель достигается решением следующих задач:

- инвентаризация активов Общества и регулярное проведение оценки рисков ИБ;

- наличие документированных процедур обеспечения ИБ, удовлетворяющих требования международного стандарта ISO 27001:2013 и Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных»;

- регулярное проведение внутреннего аудита СУИБ на соответствие внутренним нормативным документам по ИБ Общества, а также стандарту ISO 27001:2013;

- обучение работников Общества процедурам обеспечения ИБ.

4. ПРИНЦИПЫ СУИБ

4.1. В процессе обеспечения ИБ Общество должно руководствоваться принципами, приведенными ниже.

4.1.1. Законность.

При обеспечении ИБ выполняются требования законодательства РФ, а также действующие нормативные требования государственных регулирующих органов.

4.1.2. Адекватность существующим угрозам и экономическая обоснованность.

Применяемые организационные меры и технические механизмы защиты выбираются исходя из требований бизнеса на основе анализа рисков ИБ, в частности, анализа актуальных угроз и затрат на внедрение и сопровождение. Проводится периодическая оценка эффективности используемых мер и механизмов защиты.

4.1.3. Минимизация ограничивающего влияния на бизнес-процессы.

Применяемые организационные меры и технические механизмы СУИБ минимально влияют на функционирование и характеристики бизнес-процессов Общества.

4.1.4. Перспективность и ориентация на существующие российские и международные открытые стандарты.

Организационные меры и технические механизмы СУИБ реализуются с учетом мировых тенденций в области ИБ. Ориентация на открытые стандарты позволяет использовать накопленный мировой опыт в области защиты информации, а также обеспечивает единое понимание и простоту взаимодействия в рамках задач по обеспечению ИБ.

4.1.5. Непрерывность функционирования.

Обеспечивается отказоустойчивость, надежность, доступность и корректность функционирования организационных мер и технических механизмов СУИБ.

4.1.6. Непрерывность совершенствования.

Для успешного противодействия угрозам ИБ в условиях постоянно меняющегося внешнего и внутреннего окружения реализуется непрерывный цикл развития и совершенствования СУИБ.

4.1.7. Персональная ответственность.

Каждый работник Общества несет персональную ответственность за выполнение функций и требований, возложенных на него в рамках функционирования СУИБ. В случае нарушения требований ИБ работник может быть привлечен к дисциплинарной, материальной, административной, уголовной ответственности в соответствии с законодательством Российской Федерации.

4.1.8. Контроль.

Осуществляется постоянный контроль выполнения работниками Общества требований в области ИБ.

5. СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ СУИБ

5.1. Деятельность по обеспечению ИБ в Обществе должна планироваться ежегодно на уровне высшего руководства. Ресурсы на поддержку и модернизацию СУИБ должны регулярно выделяться высшим руководством.

5.2. В целях координации действий структурных подразделений Общества по обеспечению ИБ должен быть сформирован орган, выполняющий функции управления, анализа и совершенствования СУИБ - Комитет по информационной безопасности.

5.3. Ответственность за ИБ должна быть четко определена и документирована в положениях о структурных подразделениях и должностных инструкциях работников Общества.