
ПОЛИТИКА

№ _____

г. Екатеринбург

системы управления информационной
безопасностью
ОАО «Уралсвязьинформ»

Для управления процессами информационной безопасности Общества создана система управления информационной безопасностью (Далее - СУИБ) возглавляемая высшим руководством Общества.

Высшее руководство полностью отвечает за обеспечение информационной безопасности в Обществе и принимает решения по управлению СУИБ.

Цель СУИБ

СУИБ неразрывно связана с бизнес-процессом оказания инфокоммуникационных услуг и обеспечивает:

- доступность инфокоммуникационных услуг, предоставляемых Обществом;
- целостность и подлинность данных, используемых для обеспечения деятельности Общества;
- конфиденциальность информации, охраняемой в соответствии с законами Российской Федерации и локальными нормативными актами Общества;
- непрерывность бизнеса;
- минимизацию ущерба, нанесенного влиянием различных угроз информационной безопасности, бизнесу Общества;
- максимальный уровень качества и надежности предоставляемых услуг, конкурентоспособность, сохранение доброго имени и репутации компании, исполнение взятых обязательств.

Принципы построения СУИБ

Информационная безопасность (Далее - ИБ) Общества строится на основе следующих принципов:

Законность - применяемые меры ИБ не должны быть запрещены требованиями законодательства Российской Федерации, не должны наносить ущерб здоровью человека и окружающей среде;

Комплексность защиты - меры ИБ принимаются на всех участках бизнес-процесса;

Непрерывность защиты – ИБ обеспечивается непрерывно в течение всего бизнес-процесса;

Адекватность защиты – принимаемые меры ИБ адекватны имеющим место рискам;

Эргономичность защиты – применяемые меры ИБ максимально удобны для пользователей информационных систем и прозрачны для технологических систем. Должны быть максимально использованы встроенные в эксплуатируемые системы программные и аппаратные средства обеспечения информационной безопасности;

Пассивность контроля – применяемые меры ИБ не имеют непосредственного доступа к защищаемым данным и системам управления технологическим оборудованием;

Минимизация полномочий – любой участник технологического процесса имеет минимально необходимый и достаточный для исполнения должностных обязанностей набор прав и полномочий в информационных системах;

Легитимность полномочий – все операции по предоставлению доступа и назначению полномочий осуществляются на основании оформленных в установленном порядке документов (заявок);

Гарантированность восстановления – система архивирования и аудита обеспечивает возможность гарантированного восстановления системы и анализа событий, повлекших нарушение работоспособности или безопасности;

Защита инвестиций – обеспечивается полная документированность мер безопасности информационных и технологических систем на стадиях проектирования и эксплуатации;

Персональная ответственность – ответственность за нарушения требований по обеспечению информационной безопасности возлагается персонально на работника, допустившего нарушение, и соответствующего руководителя подразделения.

Основы функционирования СУИБ

Система разработана, функционирует и совершенствуется в соответствии с национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 27001-2006.

Достижение целей СУИБ и информационная безопасность Общества обеспечивается применением соответствующего комплекса организационных и

технических мер по управлению информационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного и аппаратного обеспечения.

Основой СУИБ является процесс оценки рисков информационной безопасности, согласованный с подходом к управлению рисками Общества и являющийся основой для выбора комплекса защитных мероприятий.

Степень достижения целей ИБ подлежит периодической оценке и анализу высшим руководством. Результаты анализа являются основой для назначаемых корректирующих воздействий на систему.

Для успешного функционирования системы осуществляется повышение осведомленности и постоянное обучение работников Общества вопросам информационной безопасности.

Все информационные ресурсы Общества и средства их обработки, передачи и хранения используются исключительно для достижения целей, определяемых Уставом Общества, и не могут быть использованы в целях нанесения ущерба. Недопустимо использование информационных ресурсов Общества в личных целях или в интересах третьих лиц.

Защите подлежат все информационные ресурсы Общества, средства их обработки, передачи и хранения, применяемые для осуществления производственной деятельности компании, и информационные ресурсы, применяемые Обществом для исполнения договорных или иных обязательств.

Информационная безопасность при взаимодействии с третьей стороной

Доступ работников сторонних организаций к информационным ресурсам Общества осуществляется только при условии документально оформленной договоренности о совместной защите информационных ресурсов Общества и документального подтверждения соблюдения мер ИБ в сторонней организации.

Доступ к информационным ресурсам Общества может быть предоставлен только при условии соблюдения мер обеспечения информационной безопасности.

Инфокоммуникационные услуги, оказываемые Обществом абоненту, обеспечиваются минимально необходимым уровнем информационной безопасности. Расширение применяемых мер достигается за счет предоставления абонентам Общества дополнительных сервисов и услуг информационной безопасности.

Ответственность за нарушение требований информационной безопасности

Требования Политики обязательны для исполнения всеми работниками ОАО «Уралсвязьинформ» (в том числе временными), партнерами, консультантами, клиентами Общества и третьими лицами, имеющими доступ к информационным ресурсам Общества на законных основаниях.

Каждый работник Общества обязан исполнять требования Политики и локальных нормативных документов по информационной безопасности на своем рабочем месте, при необходимости вносить предложения по ее совершенствованию.

Все инциденты информационной безопасности подлежат обязательным расследованиям, результатом которых являются адекватные корректирующие воздействия.

К работникам Общества, нарушившим требования информационной безопасности, могут применяться меры дисциплинарного взыскания в соответствии с действующим трудовым законодательством.

Сторонние организации, нарушившие требования информационной безопасности Общества, несут ответственность в соответствии с установленными гражданско-правовыми нормами.

При выявлении фактов нарушения законодательства Российской Федерации материалы расследования передаются в правоохранительные органы.

Контроль соблюдения требований Политики возлагается на заместителя генерального директора по безопасности, подразделения безопасности и руководителей филиалов Общества.