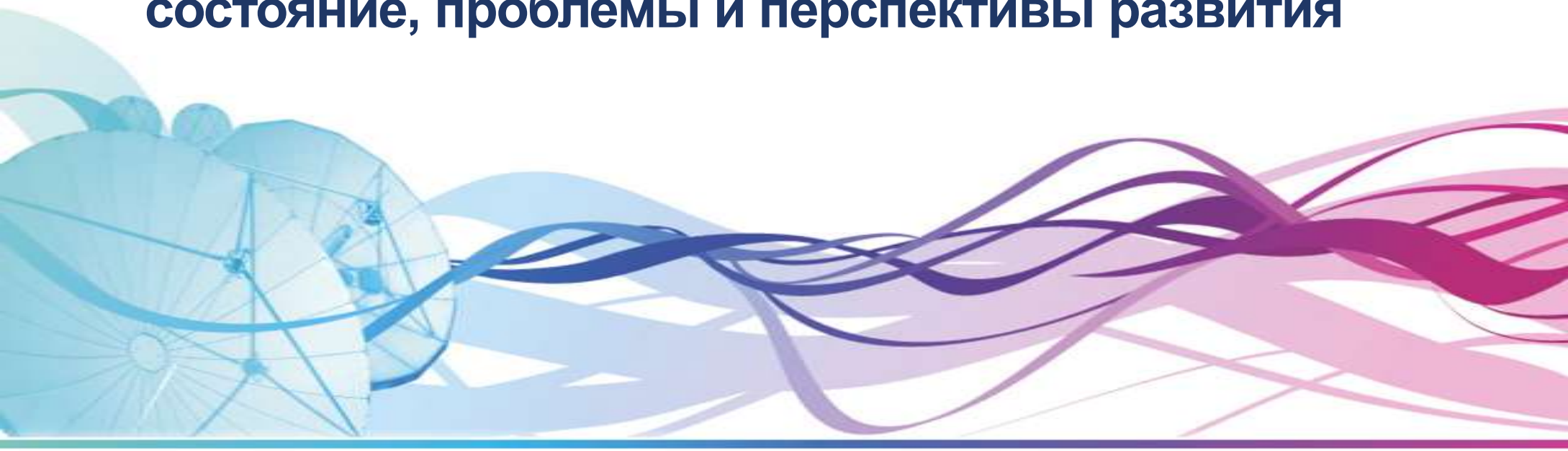
Космическая связь

Федеральное государственное унитарное предприятие

Информационная безопасность на предприятии: состояние, проблемы и перспективы развития



А.Е. Король – директор по информационным технологиям

О предприятии

- ФГУП «Космическая связь» - российский государственный оператор спутниковой связи, космические аппараты которого обеспечивают глобальное покрытие, включающее 52 страны.
- Предприятие входит в десятку крупнейших спутниковых операторов мира по объему орбитальной-частотного ресурса.
- Специалисты предприятия обеспечивают управление и мониторинг собственных спутников ГП КС, а также космических аппаратов зарубежных операторов.
- Наземная инфраструктура включает Центральный офис, Технический центр «Шаболовка» и пять Центров космической связи: «Дубна», «Медвежьи озера», «Сколково», «Хабаровск» и «Железногорск».

Цели и задачи СОИБ

Система обеспечения информационной безопасности корпоративной сети ФГУП “Космическая связь» (СОИБ) представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов предприятия от угроз информационной безопасности.

Эти меры обеспечивают:

- Доступность информации - возможность авторизованному пользователю за приемлемое время получить требуемую информационную услугу.
- Целостность информации - актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.
- Конфиденциальность информации - защита от несанкционированного доступа.

Основные принципы СОИБ

- Соответствие требованиям
- Системность
- Комплексность
- Непрерывность и актуальность
- Своевременность
- Экономическая обоснованность
- Персональная ответственность
- Разделение функций
- Минимизация прав
- Унификация
- Контроль

Объекты, подлежащие защите

- Сведения и информационные ресурсы с ограниченным доступом, составляющие коммерческую тайну, персональные данные и служебную тайну.
- Информационные системы предприятия (бухгалтерского и налогового учета, бюджетного планирования, CRM,портал, управление персоналом, базовых ИТ сервисов).
- Инфраструктура, включая технические и программные средства передачи, хранения и обработки информации, системы и средства защиты информации, здания и помещения, в которых они расположены.

Категории защищаемых информационных ресурсов

- Информация, составляющая коммерческую тайну.
- Информация, составляющая служебную тайну.
- Персональные данные сотрудников и контрагентов.
- Конфиденциальная информация (включая коммерческую тайну, служебную тайну и персональные данные), принадлежащая третьей стороне.
- Данные, критичные для функционирования ИС и работы структурных подразделений.

Структура управления ИБ

- Стратегическое управление - общее руководство организацией и контролем обеспечения ИБ. Проводится на постоянной основе Комиссией по информационной безопасности, возглавляемой первым заместителем Генерального директора.
- Оперативное управление – организация работ по обеспечению ИБ возложена на руководителя службы информационных технологий. Методическое руководство и контроль над эффективностью предусмотренных мер защиты информации возложено на главного специалиста по ИБ предприятия.
- Административное управление – реализация процессов обеспечения ИБ, администрирование и управление средствами обеспечения ИБ возложена на назначенных ответственных в центральном офисе и филиалах предприятия.

Меры обеспечения ИБ

- Организационные (административный уровень и процедуры).
- Физические.
- Программно-технические.

Организационные меры

Административный уровень представлен документами:

- «Политика информационной безопасности предприятия».
- «Стратегия информационной безопасности предприятия».
- «Модели угроз и модели нарушителя информационной безопасности».

Процедурные методы защиты информации определяются локальными нормативными документами, разрабатываемыми на основе утвержденной политики безопасности.

Физические меры

- Здания (охрана, видеонаблюдение).
- Помещения (сигнализация, замки, электронные пропуска с разграничением допуска).
- Для хранения конфиденциальных документов и машинных носителей с защищаемой информацией, помещения снабжаются сейфами и металлическими шкафами.

Программно-технические меры

- Идентификация и аутентификация пользователей.
- Разграничение доступа.
- Протоколирование и аудит действий пользователей.
- Межсетевое экранирование.
- Шифрование информационных потоков критической информации.
- Антивирусная защита и профилактика серверного и пользовательского оборудования.
- Фильтрация нежелательного веб-трафика.
- Защита от нежелательной почты.
- Фильтрация сетевых пакетов по их содержимому.
- Контроль защищенности ИС.

Факторы, влияющие на появление новых проблем

- Расширение информационного взаимодействия предприятия с контрагентами, в т.ч. при обслуживании программно-технических средств.
- Значительное расширение сферы использования автоматизированных систем, увеличение их количества, сложности, наличие разнообразных интеграционных связей между ними.
- Активное использование сотрудниками предприятия в работе мобильных устройств за пределами контролируемой зоны.
- Рост объемов информации, передаваемой по открытым каналам связи.
- Новые виды угроз и атак.
- Недостаточная осведомленность в вопросах ИБ работников предприятия.

Перспективы развития

- Доработать процедуры проведения восстановительных работ при возникновении аварий, которые позволят уменьшить ущерб и обеспечить быстрое восстановление функционирования автоматизированных бизнес-процессов предприятия.
- На регулярной основе проводить тренинги сотрудников предприятия по информационной безопасности.
- В части контроля защищенности ИТ инфраструктуры предприятия от угроз ИБ организовать на периодической основе проведение аудита безопасности ИС, контроль выполнения правил утвержденных политик безопасности администраторами и пользователями корпоративной сети, контроль за использованием мобильных устройств.
- В части предотвращения, выявление, реагирования и расследования нарушений ИБ автоматизировать процессы сбора и управления событиями ИБ.
- В части усиления контроля над действиями внешних исполнителей ограничить число шлюзов и внедрить единую систему управления доступа.

Космическая связь
Федеральное государственное унитарное предприятие

Спасибо за внимание!

А.Е. Король
akorol@rscc.ru