Управление информационной безопасности

Проект по целям и задачам Управления

УКЗ

Основная цель Отдела защиты информации.

Целью руководства Общества в области информационной безопасности является обеспечение защиты информации от внешних и внутренних угроз, предотвращение или минимизация возможных потерь и ущерба от нарушений для стабильного и эффективного функционирования деятельности Общества.

- Обеспечивать соблюдение требований, установленных законодательством Российской Федерации, ПАО «Газпром нефть» в области информационной безопасности;
- Обеспечивать реализацию организационных и технических мероприятий по защите ИТ-инфраструктуры, корпоративной информационно-вычислительной системы Общества, объектов критической информационной инфраструктуры;
- Обеспечивать безопасность собственной информации, а также информации, доверенной Обществу контрагентами в рамках договорных или иных обязательств;
- Проводить работы с контрагентами, осуществляющими деятельность в интересах ПАО «Слафнефть-мегионнефтегаз» по соблюдению требований правовых актов, нормативных документов федерального и корпоративного уровней в области информационной безопасности;
- Осуществлять оценку рисков в области информационной безопасности, обеспечивать управление рисками для предупреждения возникновения угроз информационной безопасности;
- Обеспечивать выявление потенциальных угроз информационной безопасности;
- Осуществлять мероприятия, направленные на повышение культуры информационной безопасности работников Общества;
- Поддерживать и повышать профессиональную компетентность работников, ответственных за обеспечение информационной безопасности в Обществе;
- Направлять необходимые ресурсы для реализации обязательств настоящей Политики.

Фокус внимания

В условиях сложившейся геополитической обстановки, показывает что зарубежными хакерскими группировками при реализации компьютерных атак на информационную инфраструктуру РФ активно эксплуатируются уязвимости программного обеспечения.

С целью предотвращения реализации угроз безопасности информации и оперативного реагирования, связанных с эксплуатацией уязвимостей, а так же проведением сканирования сети на факт скрытых подсетей и точек доступа WI-FI в Обществе необходимо на регулярной основе выполнять следующие мероприятия:

- Регламентированное проведение периодических инвентаризаций общедоступных информационных ресурсов (веб-сайтов, порталов), с целью определения сетевых служб, открытых на периметре систем и сетей, а также сканирование IP-адресов, выделенных для систем и сетей в арендованном облаке/хостинге с целью отключения неиспользуемых служб и веб-сервисов.
- Анализ открытых портов для определения принадлежности и легитимности доступных по открытым портам сервисов и последующая блокировка доступа извне к сетевым службам.
- Проведение инвентаризации систем и сетей на предмет наличия отдельных каналов управления программным обеспечением и оборудованием. В том числе, выявления каналов, построенных с использованием 3G/LTE оборудования и расширяющие поверхность реализации компьютерных атак.
- Поиск и отключение не легитимных точек доступа Wifi.
- Анализ трафика прикладного уровня – противодействие сканированию сети и выявление внутренних нарушителей.
- Контроль за использованием учетных записей на сетевом оборудовании (запрет на создание, модификацию, удаление не легитимных УЗ).
- Мониторинг выполнения служебными (сервисными) учетными записями команд, не типичных для служб, к которым они относятся
- Осуществление сбора и мониторинга событий создания SSH-тоннелей и проброса портов. потенциальных риск получения злоумышленником доступа к сетевому оборудованию
- Осуществление сбора и мониторинга событий изменения файлов /etc/passwd, /etc/shadow.

Невыполнение вышеуказанных мероприятий несет высокий риск утечки информации по техническим каналам связи или выведение из строя корпоративной сети ПАО «СН-МНГ», что ведет за собой остановку фонда нефтедобычи, либо прерывания в работе АСУ ТП на неопределенное время.

Обоснование по изменению Отдела защиты информации.

В условиях сложившейся геополитической обстановки от Федеральной службы по техническому и экспортному контролю (ФСТЭК России) получено большое количество задач для выполнения на регулярной основе следующих мер контроля на Объектах КИИ (ФЗ-187)

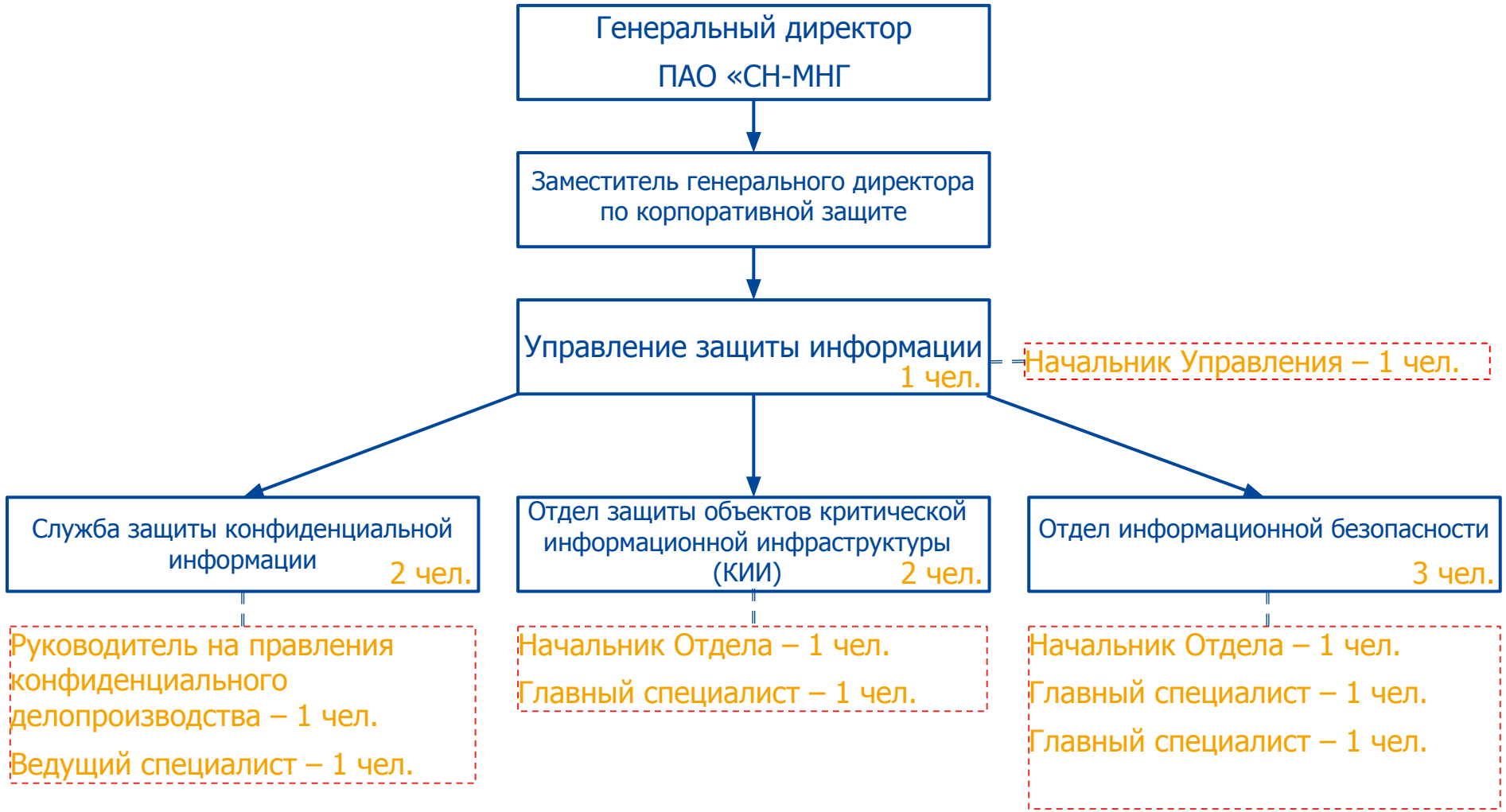
- Контроль обслуживания АРМ и серверов объектов КИИ в части ИБ
- Контроль средств АВЗ объектов КИИ
- Контроль систем защиты от несанкционированного доступа объектов КИИ
- Контроль обслуживания серверов баз банных объектов КИИ
- Контроль систем идентификации, аутентификации и управления доступом пользователей объектов КИИ
- Контроль систем ограничений программной среды объектов КИИ
- Контроль системы установки обновлений ПО объектов КИИ
- Контроль систем резервного копирования информации на объектах КИИ
- Контроль ограничений использования съемных устройств на объектах КИИ
- Проведение анализа функционирования системы безопасности и состояния безопасности объектов КИИ. По результатам анализа осуществление разработки предложений по развитию системы безопасности и мер по совершенствованию безопасности объектов КИИ с участием эксплуатирующих и обеспечивающих функционирование структурных подразделений Общества.
- На регулярной основе проводить выезды на месторождения с целью выявления и предотвращения Легкодоступных подключений к каналам связи АСУ ТП на Кустовой площадке, а так же ДНС, КНС.

Невыполнение вышеуказанных мероприятий несет высокий риск утечки информации по техническим каналам связи или выведение из строя корпоративной сети ПАО «СН-МНГ», что ведет за собой остановку фонда нефтедобычи, либо прерывания в работе АСУ ТП на неопределенное время.

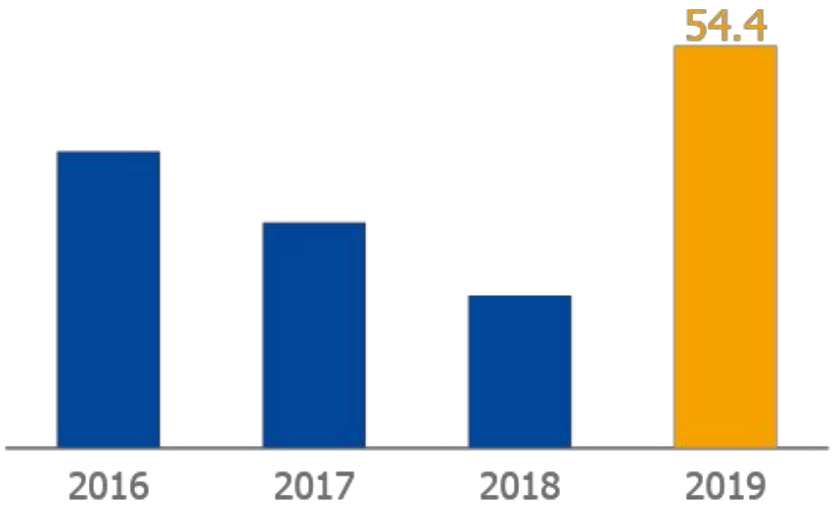
Обоснование по реорганизации Отдела защиты информации

Для выполнения и усиления мер по информационной безопасности предлогаю провести реорганизацию Отдела защиты информации, это приведет к выполнению задач по направлению каждого отдела, а так же закреплением ответственных по обеспечению Критической информационной

Структурный план по отделам и службам в Управлении ИБ



Заголовок



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut **consectetur magna** nec nulla aliquam tristique.

- Duis a odio luctus, auctor libero vitae, congue odio.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut **consectetur magna** nec nulla aliquam tristique.

- Duis a odio luctus, auctor libero vitae, congue odio.

Заголовок

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut **consectetur magna** nec nulla aliquam tristique.

- Duis a odio luctus, auctor libero vitae, congue odio.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut **consectetur magna** nec nulla aliquam tristique.

- Duis a odio luctus, auctor libero vitae, congue odio.