Категорирование и требования безопасности к ЗОКИИ

Рудаш Андрей, CISSP
Дирекция по информационной безопасности ПАО «ВымпелКом»

Билайн

Содержание

Критические процессы	Показатели значимости
1. Управление и эксплуатация услуг связи 2. Управление и эксплуатация ресурсов для услуг связи	1. Прекращение или нарушение функционирования сети связи 2. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия) 3. Возникновение ущерба бюджетам Российской Федерации

Ключевые услуги

Ключевая услуга	Сервис
Мобильный Голос	Голос Роуминг
Мобильный интернет	Интернет
Digital	Личный кабинет (Система самообслуживания абонентов)
Фикс голос	Голос Услуги международной, междугородной и внутризоновой телефонной связи
Фикс интернет	Internet FTTB IP VPN IPTV FTTB

Ключевые ресурсы

1. Проанализированы информационные и телеком системы.
2. Определены зависимости услуг от ИТ и телеком систем.
3. Выделены ИС, ИТС, АСУ <u>непосредственно</u> влияющие на услуги связи.

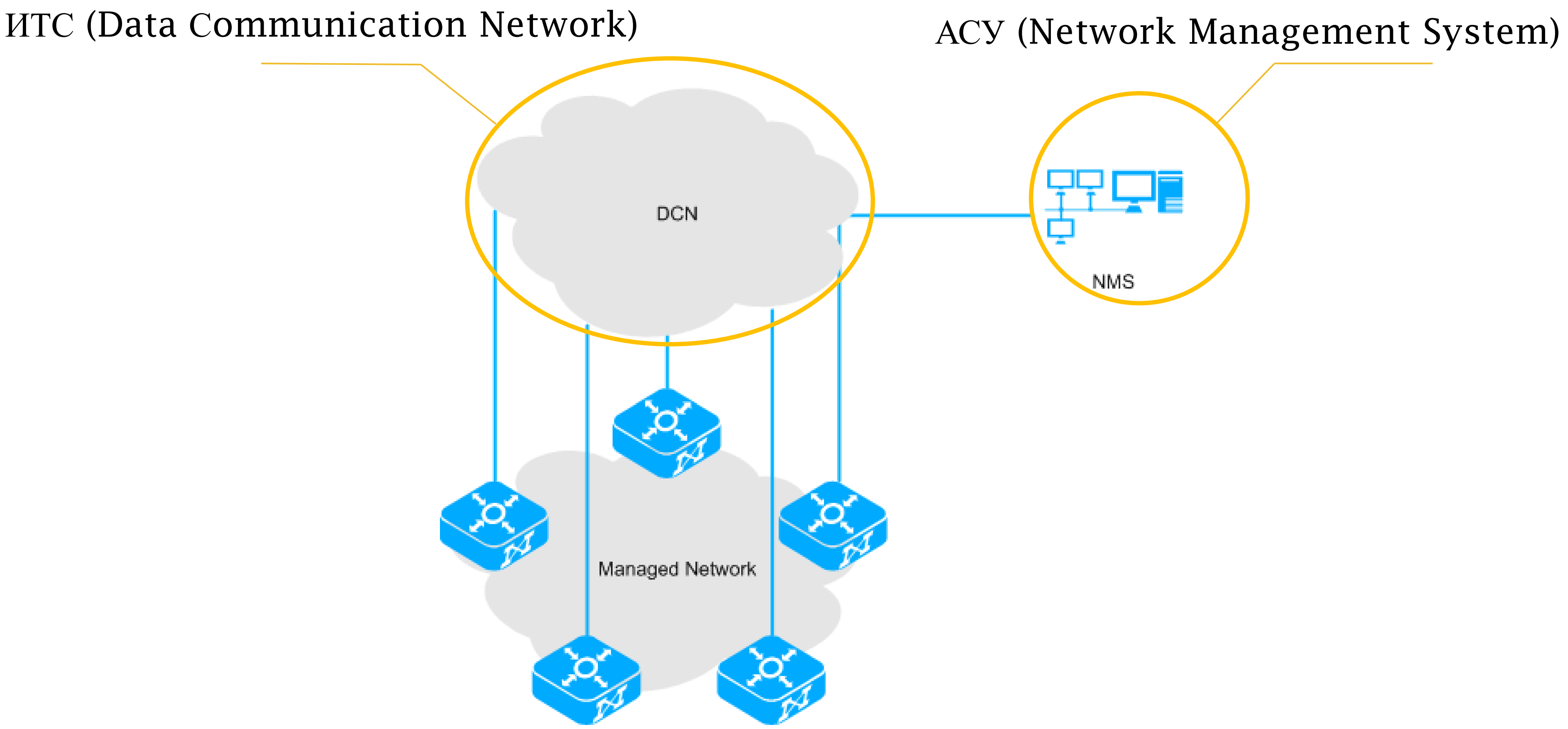
Статистика по объектам КИИ для категорирования

1. Информационные системы - 17

2. Автоматизированные системы управления – 48

3. Информационно телекоммуникационная сеть - 1

АСУ и ИТС



ИТС (Data Communication Network)
АСУ (Network Management System)
DCN
NMS
Managed Network

СЗИ ЗОКИИ

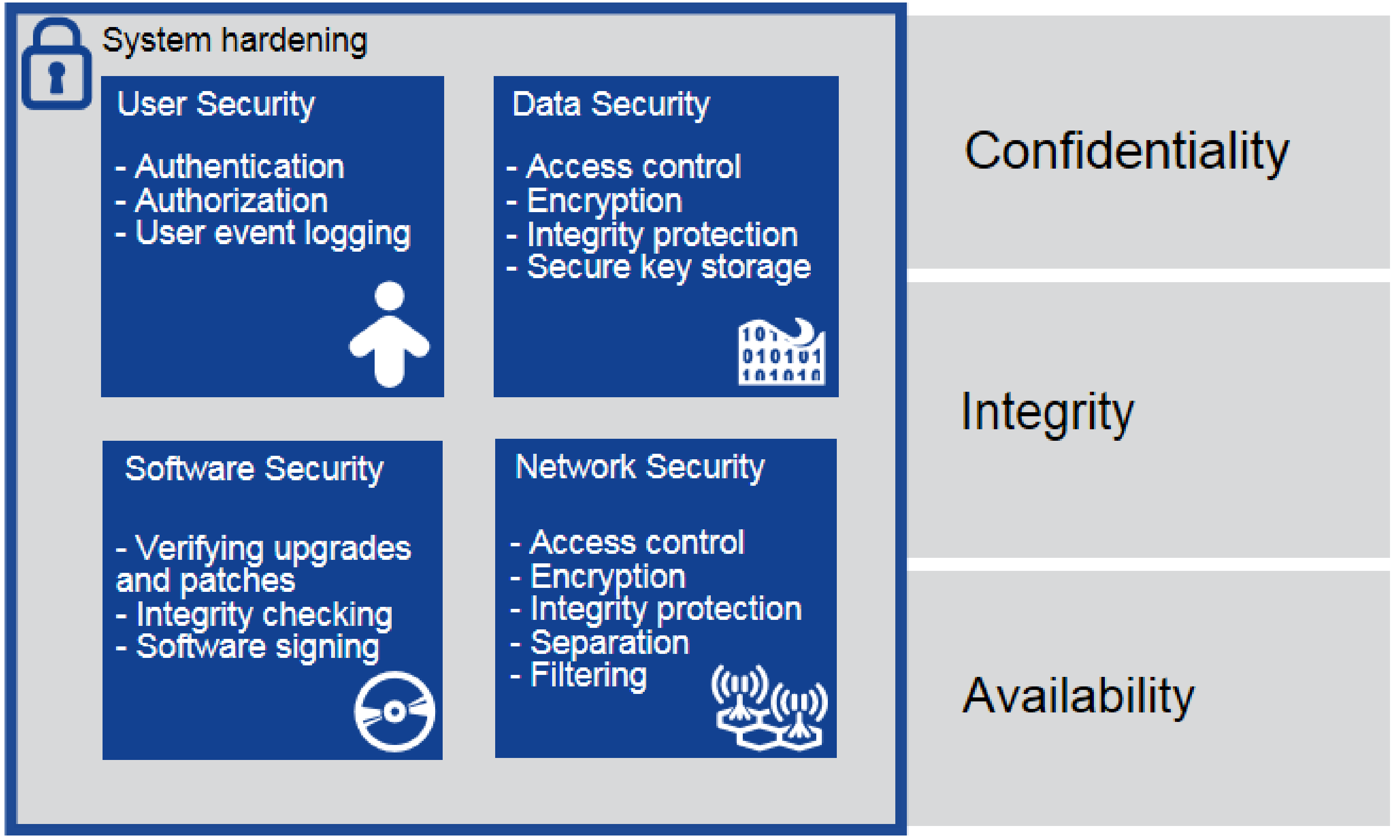
- Для значимых объектов, находящихся в эксплуатации, требования безопасности к ЗОКИИ подлежат реализации в рамках модернизации или дооснащения подсистем безопасности эксплуатируемых значимых объектов.

- «…в приоритетном порядке подлежат применению СЗИ, встроенные в ПО или программно-аппаратные средства объектов»;

- При отсутствии возможности реализации отдельных мер по обеспечению безопасности и (или) невозможности их применения к отдельным объектам и субъектам доступа, в том числе вследствие их негативного влияния на функционирование значимого объекта в проектных режимах значимого объекта, должны быть разработаны и внедрены компенсирующие меры, обеспечивающие блокирование (нейтрализацию) угроз безопасности информации с необходимым уровнем защищенности значимого объекта.

- Для обеспечения безопасности ЗОКИИ должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

Встроенные сервисы безопасности NMS



Источник: Nokia

Типовой комплект документов для системы защиты ЗОКИИ.

1. Модель угроз безопасности ЗОКИИ
2. Акт категорирования ЗОКИИ
3. Техническое задание на создание системы защиты ЗОКИИ
4. Проект создания системы защиты ЗОКИИ (выбор окончательных решений)
5. Программа и методика оценки соответствия СЗИ ЗОКИИ требованиям безопасности (учитываем ГОСТ Р ИСО/МЭК 15408, требования НПА, модели угроз)
6. Протокол оценки соответствия СЗИ ЗОКИИ требованиям безопасности
7. Заключение по результатам оценки соответствия СЗИ ЗОКИИ требованиям безопасности.

Аутсорсинг эксплуатации сети оператора связи и требования к ЗОКИИ

Приказ ФСТЭК России №239

……

31. В значимом объекте не допускаются:

наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры;

наличие локального бесконтрольного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры;

Аутсорсинг эксплуатации сети оператора связи и требования к ЗОКИИ

1. Устанавливаются требования по контролю действий и управлению доступом третьих лиц при осуществлении удаленного доступа к программному и программно-аппаратному обеспечению значимых объектов критической информационной инфраструктуры.

2. При этом возможность технической поддержки программного и программно-аппаратного обеспечения иностранными производителями не исключается, но должно осуществляться под контролем субъекта критической информационной инфраструктуры.

Аутсорсинг эксплуатации сети оператора связи и требования к ЗОКИИ

Требования ИБ к процессу аутсорсинга на значимых объектах КИИ:

1. Требования безопасности должны быть прописаны в договорах и контрактах на проведение работ или оказание услуг на всех этапах жизненного цикла значимых объектов КИИ.
2. Между оператором и аутсорсером должно быть согласовано разделение обязанностей за обеспечение безопасности.
3. Все сотрудники внешней компании должны подписывать соглашение о конфиденциальности, включающее требование о соблюдении конфиденциальности информации доверенной сотруднику или ставшей известной ему входе исполнения должностных обязанностей.
4. Субъект КИИ должен внедрить технические решения по мониторингу и контролю (удаленного, локального) доступов сотрудников сторонних организаций.
5. Субъект КИИ должен осуществлять мониторинг выполнения аутсорсинговых соглашений в части требований ИБ.

Спасибо за внимание