РУСЭНЕРГОСБЫТ

Васьковский Андрей Сергеевич

Начальник департамента ИБ ООО «Русэнергосбыт»

Обеспечение информационной безопасности в энергосбытовых компаниях

ООО «Русэнергосбыт» создано в 2002 году, осуществляет деятельность в 69 регионах, гарантирующий поставщик электроэнергии в 17 регионах

Структура компании включает в себя 8 филиалов:

Филиал в республике Татарстан (Казань)
Тюменский филиал (Новый Уренгой)
Восточно-Сибирский филиал (Иркутск)
Приволжский филиал (Саратов)
Горьковский филиал (Нижний Новгород)
Северный филиал (Ярославль)
Западно-Сибирский филиал (Новосибирск)
Октябрьский филиал (Санкт-Петербург)

Среди клиентов компании: ОАО «РЖД», ОАО «КАМАЗ», ОАО «Соллерс», предприятия «Группы ГАЗ», ГК «Air Liquide», ОАО «Силовые машины», InBev, ОАО «Волжский оргсинтез» и т.д.

Почему ИБ критична для энергосбытовых компаний?

Энергосбытовая деятельность — часть критической инфраструктуры государства.

Риски: кибератаки на системы учёта энергии, утечки персональных данных клиентов, остановка работы биллинговых систем.

Последствия: финансовые потери, репутационные риски, сбои в энергоснабжении.

Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры»

Перечень отраслей, которые входят в критическую информационную инфраструктуру (КИИ) согласно 187-ФЗ, включает:
здравоохранение; наука; транспорт; связь; **энергетика;** банковская сфера и иные финансовые сферы; топливно-энергетический комплекс; область атомной энергии; оборонная промышленность; ракетно-космическая промышленность; горнодобывающая промышленность; металлургическая промышленность; химическая промышленность.

Ключевые риски:

Кибератаки (DDoS, ransomware, APT-атаки, хактивисты).

Утечки данных клиентов (персональные данные, платёжная информация).

Внутренние угрозы (ошибки сотрудников, умышленные действия).

Уязвимости IoT-устройств (умные счётчики (интеллектуальная система учета)).

Интеллектуальная система учёта электроэнергии (ИСУЭ) — объект критической информационной инфраструктуры (КИИ).
Это утверждение содержится в перечне типовых отраслевых объектов КИИ, работающих в области энергетики.
Ключевое негативное последствие инцидента в ИСУЭ — несанкционированное отключение электроэнергии, основная категория значимости — «Социальная значимость».
Работа ИСУЭ регулируется, в частности, Постановлением Правительства РФ от 19.06.2020 №890.

Показатели социальной значимости и их значения для разных категорий:

Категорирование объектов КИИ

Определение критических процессов

Социальная значимость

Показатели критериев значимости	Значение показателя		
	III категория	II категория	I категория
Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500
Прекращение[1] или нарушение функционирования[2] объектов обеспечения жизнедеятельности населения, оцениваемые:			
а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	в пределах территории одного муниципального образования (численностью от 2 тыс. чел.) или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования (численностью от 2 тыс. чел.) или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения
б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	более или равно 2, но менее 1 000	более или равно 1 000, но менее 5 000	более или равно 5 000

Процедура присвоения категории

Создание комиссии:
Руководитель субъекта КИИ формирует комиссию, включающую специалистов по ИБ, технологическим процессам и гражданской обороне.

Анализ процессов:
Выявляются критические процессы (например, управление энергосетями) и связанные с ними объекты КИИ.

Оценка последствий:
Используются таблицы из Постановления №127, где для каждого показателя указаны пороговые значения (например, количество пострадавших или длительность простоя).

Направление документов во ФСТЭК:
Результаты категорирования оформляются актом и отправляются в ФСТЭК в течение 10 дней. Регулятор проверяет данные и может потребовать исправлений.

Категорирование объекта КИИ

Объекты ИСУЭ должны быть отнесены к одной из категорий значимости (I, II, III) в зависимости от потенциального ущерба при нарушении их работы. Например, системы, влияющие на электроснабжение больниц или очистных сооружений, автоматически получают высшую категорию 110.

Реализация технических мер защиты

Контроль физического доступа.
Криптографическая защита (СКЗИ).
Резервирование и автономность.
Межсетевое экранирование.
Антивирусная защита и обновления.

Импортозамещение

С 2025 года запрещено использование иностранного ПО и оборудования на значимых объектах КИИ.
Для ИСУЭ требуется переход на российские решения, такие как ОС Astra Linux, СУБД Postgres Pro и ПО «Пирамида 2.0» 57.
Обязательна сертификация средств защиты информации (например, ФСТЭК и ФСБ)

Цели информационной безопасности

Обеспечение бесперебойной работы систем. Недопущение сбоев в работе на оптовом рынке электроэнергии

Защита персональных данных потребителей.

Соответствие требованиям регуляторов (ФЗ-152, ФЗ-187, ГОСТ Р 57580).

Минимизация финансовых и репутационных потерь.

Нормативная база
Основные документы:
ФЗ-187 «О безопасности критической информационной инфраструктуры».
ФЗ-152 «О персональных данных».
ГОСТ Р 57580 (требования к ИБ в энергетике).

Методы защиты

Технологические решения:
Внедрение межсетевых экранов **NGFW (Next-Generation Firewall)** и систем обнаружения вторжений (IDS/IPS).

Шифрование данных при передаче и хранении.

Резервное копирование и аварийное восстановление (DRP).

Организационные меры:

Разработка политики ИБ и регламентов.
Регулярное обучение сотрудников.
Проведение пентестов или bug bounty и аудитов.

Паспорт объекта КИИ — это обязательный документ, содержащий информацию об объекте, его значимости, уязвимостях и мерах защиты. Он формируется в рамках процедуры категорирования и служит основой для выполнения требований ФЗ №187 «О безопасности КИИ».

Назначение паспорта КИИ

•Фиксация категории значимости объекта (I, II, III) на основе социальных, экономических и политических последствий его нарушения.

•Определение перечня информационных систем, сетей и процессов, относящихся к КИИ.

•Планирование и обоснование мер защиты в соответствии с требованиями регуляторов (ФСТЭК, ФСБ).

4. Ответственность за отсутствие паспорта

Административные штрафы (ст. 13.12 КоАП РФ):

Для юрлиц: до 500 тыс. рублей.

Для должностных лиц: до 50 тыс. рублей.

Уголовная ответственность (ст. 274.1 УК РФ):

Если отсутствие паспорта привело к тяжелым последствиям (жертвы, экологическая катастрофа).

Структура паспорта (основные разделы)

Общие сведения:

Наименование объекта, юридический адрес, реквизиты владельца.

Перечень ответственных лиц (руководитель, специалист по ИБ).

Дата создания и срок актуальности документа.

Категория значимости:

Уровень значимости (I, II, III) с указанием критериев (социальные, экономические, политические последствия).

Обоснование присвоенной категории (например, потенциальный ущерб для 1 млн человек при остановке работы).

Описание информационной инфраструктуры:

Схема технологических процессов и связанных с ними информационных систем (например, АСУ ТП энергосетей).

Перечень используемого ПО, оборудования, каналов связи.

Угрозы и уязвимости:

Результаты анализа рисков (например, уязвимости в SCADA-системах).

Список актуальных угроз (кибератаки, саботаж, ошибки персонала).

Меры защиты:

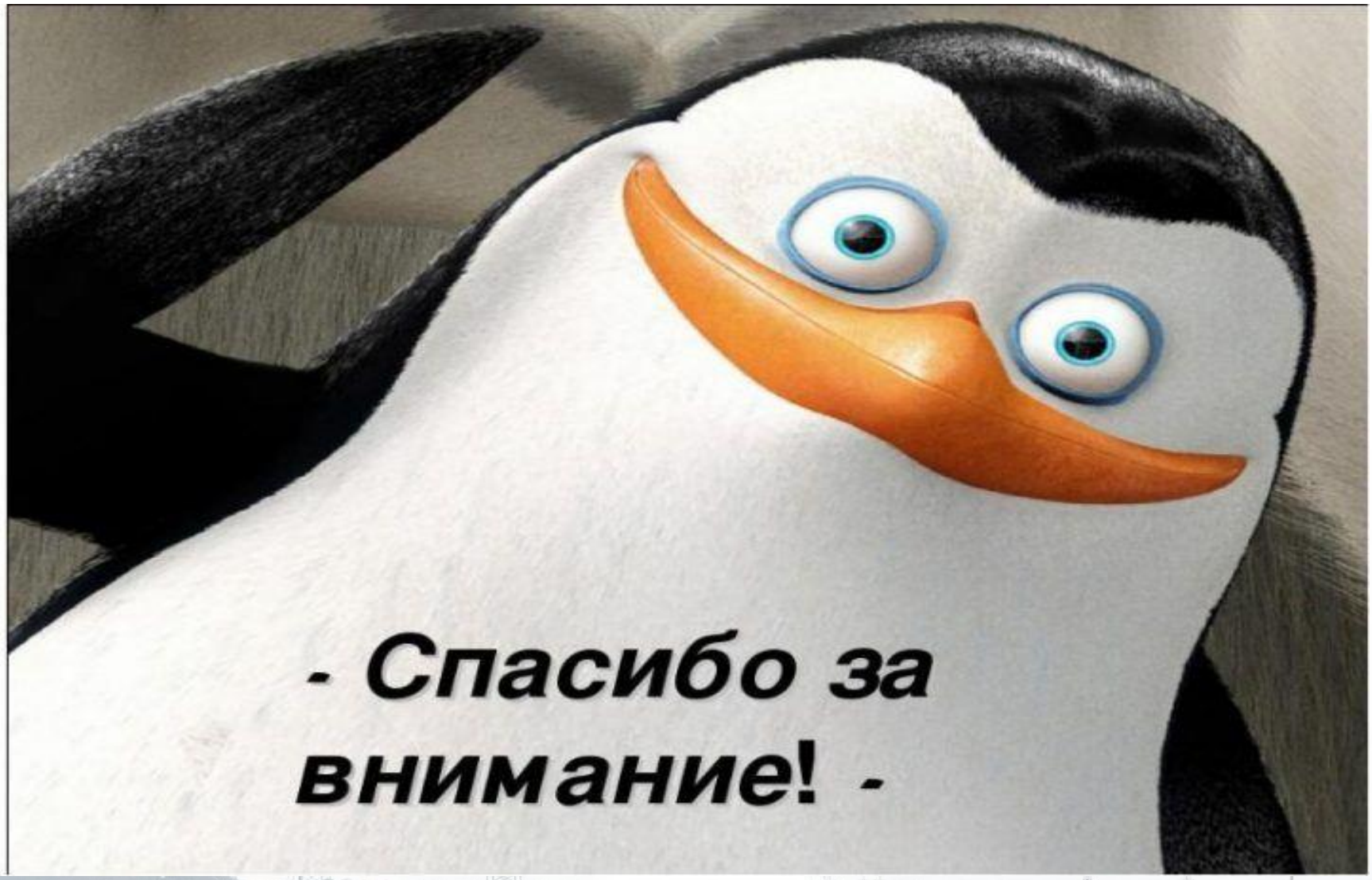
Внедренные и планируемые средства защиты (например, СЗИ, сертифицированные ФСТЭК).

Политики доступа, системы мониторинга (SIEM), резервное копирование.

План реагирования на инциденты.

Приложения:

Копии актов категорирования, протоколов проверок, заключений комиссии.


- Спасибо за внимание! -