Смена парадигмы: от обеспечения к управлению информационной безопасностью в электроэнергетике

Литвинов Павел Васильевич

заместитель председателя секции IT НП «НТС ЕЭС», эксперт РНК СИГРЭ

Оглавление

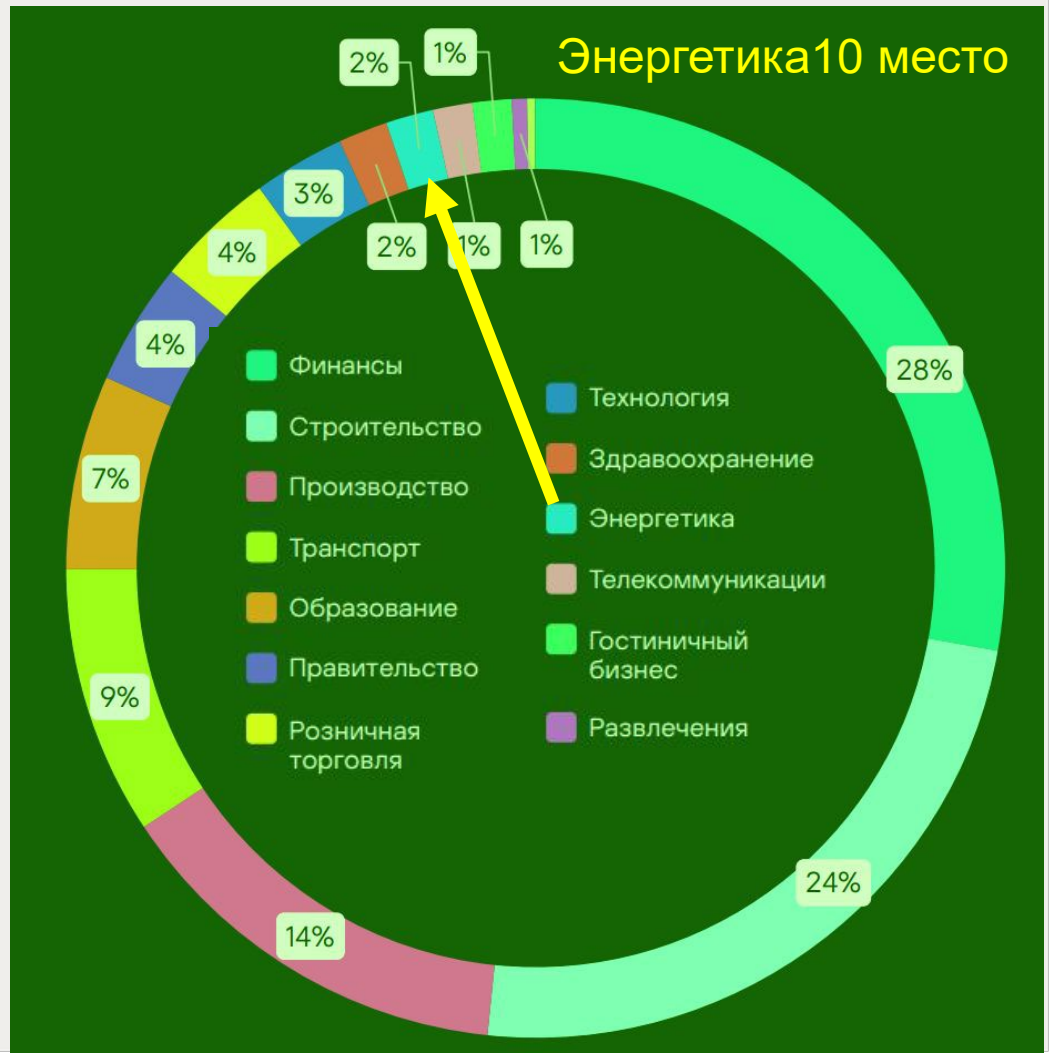
1. Текущее состояние ландшафта киберугроз
2. Существующие меры противодействия
3. Новеллы в законодательстве
4. Пример динамичного изменения ситуации
5. Типичные ошибки при планировании ИБ
6. Как их избежать с учетом мирового опыта
7. Новая парадигма – от обеспечения к управлению ИБ
8. Процессы управления информационной безопасностью
9. Практические рекомендации

cigre
For power system expertise

Распределение числа атак по секторам* в 2024 г.

- Энергетика по числу атак находится на 10-ом месте это «всего» 2 %
- Число атак не отражает уровень серьезности и стоимость последствий
- Информация не может быть полной о числе, не говоря уж об ущербе
- Продвинутые APT атаки могут готовиться и длиться годами
- Наблюдаются положительная динамика в ресурсном обеспечении, разнообразии способов и количестве атак:
  - политически мотивированный хактивизм
  - кооперация хакерских группировок
  - вовлечение «втемную» через продажу или распространение вредоносного ПО
  - участие спецслужб недружественных стран

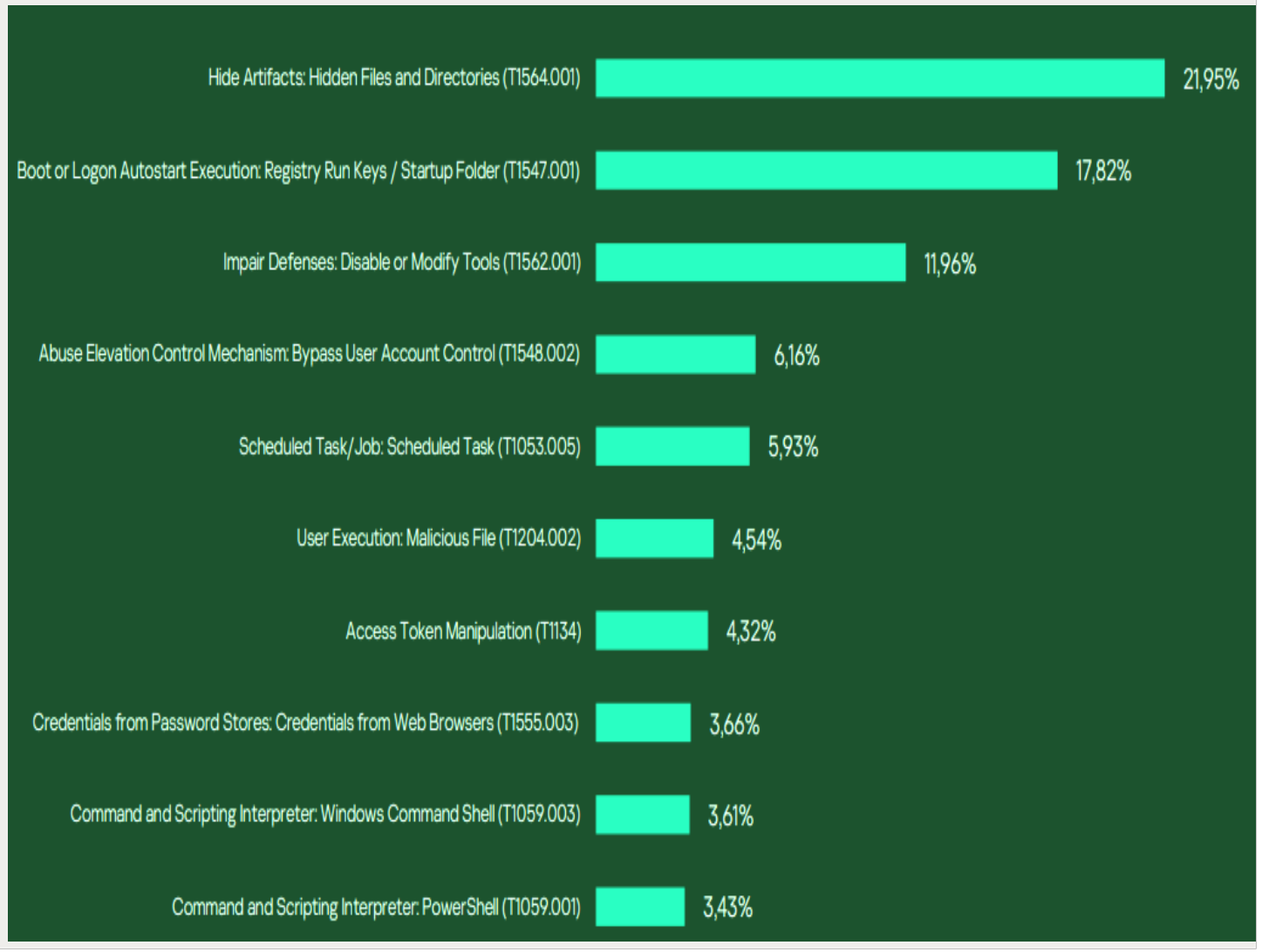
В отрасли удалось обеспечить адекватное противодействие но успокаиваться рано.



*Источник: Аналитический отчет Лаборатории Касперского «Ландшафт киберугроз», 2024 г.

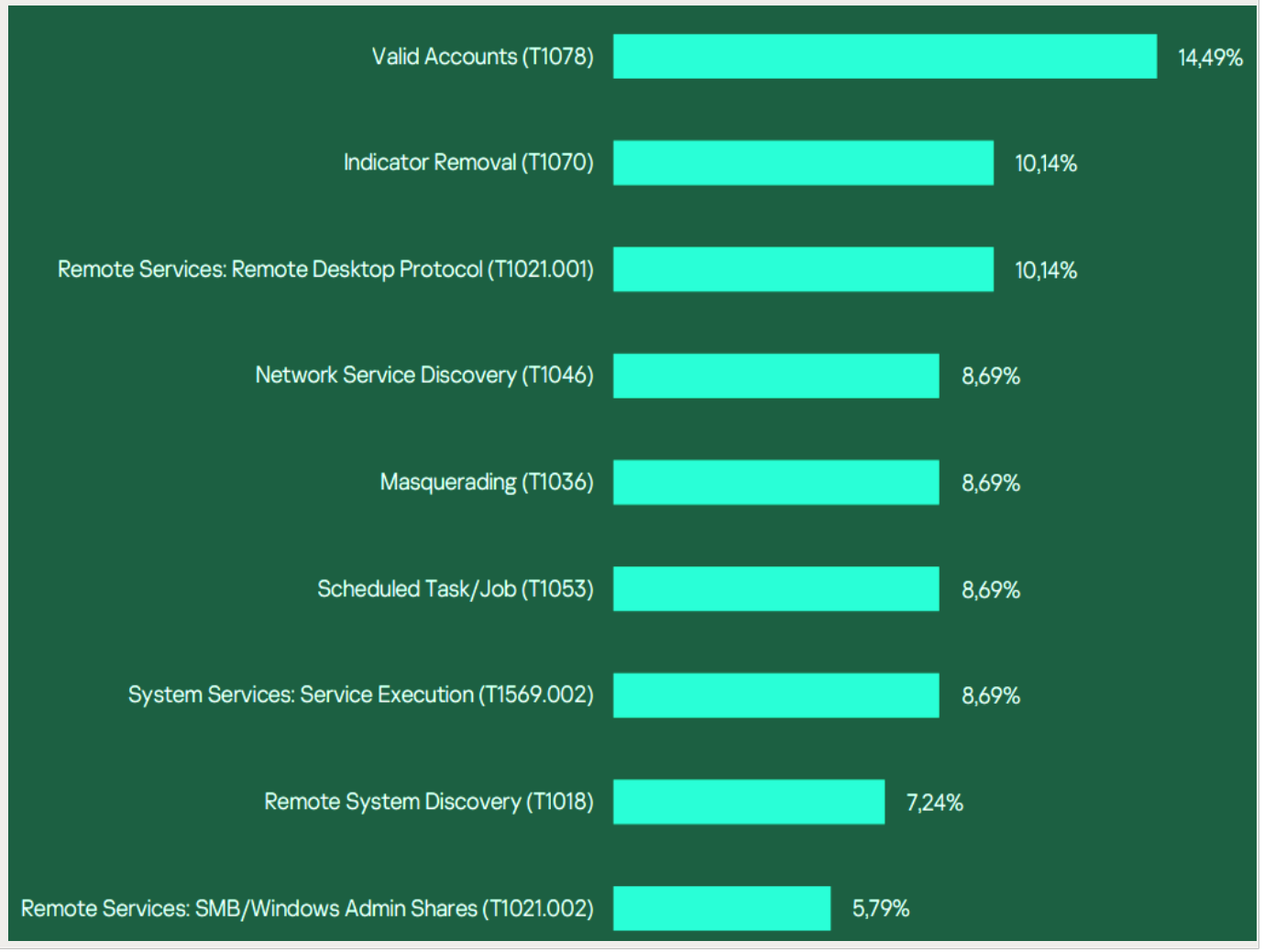
Популярные векторы атак

- Скрытые артефакты (файлы и директории)
- Добавление в автозапуск или изменение ключей реестра
- Модификация или отключение инструментов безопасности
- Обход контроля учетных записей
- Использование планировщика задач Windows
- Пользователь открывает вредоносный файл (социальный инжиниринг)



Техники атак (расследованные инциденты)

- Использование действительной учетной записи
- Скрытие присутствия в системе
- Использование удаленного рабочего стола
- Сканирование сетевой инфраструктуры для поиска устройств и уязвимостей
- Маскировка вредоносных артефактов и обман пользователей
- Использование планировщика задач для регулярного запуска вредоносного кода



Мотивация и цели атакующих, основные виды угроз

- **Финансовые**
  - блокировка доступа к данным с целью выкупа
  - кража с целью перепродажи
- **Политические**
  - шпионаж и сбор разведданных
  - влияние на политические процессы, манипулирование общественным мнением

- шифровальщики
- утечки данных в даркнет
- фишинговые атаки или социальная инженерия
- **эксплуатация уязвимостей в ПО**

Место	Продукт	Тип уязвимости	Оценка CVSS
1	Версии 7-Zip ранее 23.00	Выполнение вредоносного кода	7.8
2	7-Zip 21.07 и более ранние версии	Повышение привилегий Выполнение вредоносного кода	7.8
3	WinRAR 6.x ранее версии 6.23	Выполнение вредоносного код	7.8
4	Google Chrome ранее версии 112.0.5615.50	Выполнение вредоносного кода. Отказ в обслуживании. Обход системы безопасности. Повышение привилегий	8.8

Как давно вы обновляли 7-zip и WinRAR?

Законодательство и меры противодействия

- ФЗ и Приказы ФСТЭК
- Требования по шифрованию ФСБ
- Классификация объектов КИИ
- Создание центров ГосСОПКА и НКЦКИ
- Импортозамещение
- Статическое и динамическое тестирование ПО
- Сертификация и аттестация

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен Советом Федерации 19 июля 2017 года

Статья 1. **Сфера действия настоящего Федерального закона**

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Статья 2. **Основные понятия, используемые в настоящем Федеральном законе**

Для целей настоящего Федерального закона используются следующие основные понятия:

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 50524
от "26" марта 2018 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)

ПРИКАЗ

«25» декабря 2017 г. Москва № 239

Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю**:

Утвердить прилагаемые Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Министерство энергетики Российской Федерации
(Минэнерго России)

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 53815
от "12" февраля 2019 г.

ПРИКАЗ

6 ноября 2018 г. № 1015

Москва

Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования

В соответствии с подпунктом «б» пункта 1 постановления Правительства Российской Федерации от 2 марта 2017 г. № 244 «О совершенствовании требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики и внесении изменений в некоторые акты Правительства Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 11, ст. 1562; 2018, № 34, ст. 5483) п р и к а з ы в а ю:

1. Утвердить прилагаемые требования в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования.

2. Настоящий приказ вступает в силу по истечении шести месяцев со дня его официального опубликования.

Министр А.В. Новак

Департамент оперативного контроля и управления в электроэнергетике
Медведева Елена Анатольевна
(495) 631-88-71

Судя по датам документов законодательная база готовилась давно и это работает

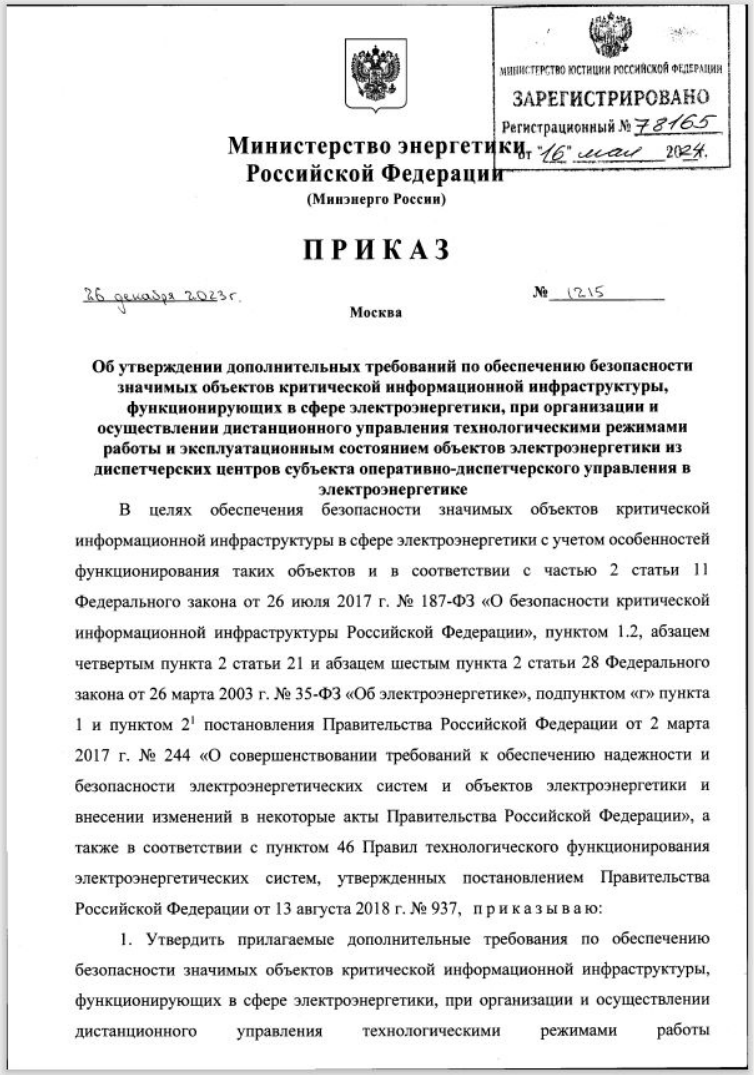
Новеллы законодательства

- приказ* Минэнерго от 26.12.2023 № 1215 «Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике»

- Вступает в силу с 1 сентября 2024 г. действует до 1 сентября 2030 г.

- Цель: устанавливает требования по защите трафика команд дистанционного управления средствами криптографической защиты. Выбор класса в зависимости от модели угроз.

*Полный текст (12 стр.)



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 78165
от "16" мая 2024

Министерство энергетики Российской Федерации
(Минэнерго России)

ПРИКАЗ

26 декабря 2023 г. № 1215

Москва

Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике

В целях обеспечения безопасности значимых объектов критической информационной инфраструктуры в сфере электроэнергетики с учетом особенностей функционирования таких объектов и в соответствии с частью 2 статьи 11 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», пунктом 1.2, абзацем четвертым пункта 2 статьи 21 и абзацем шестым пункта 2 статьи 28 Федерального закона от 26 марта 2003 г. № 35-ФЗ «Об электроэнергетике», подпунктом «г» пункта 1 и пунктом 2^1 постановления Правительства Российской Федерации от 2 марта 2017 г. № 244 «О совершенствовании требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики и внесении изменений в некоторые акты Правительства Российской Федерации», а также в соответствии с пунктом 46 Правил технологического функционирования электроэнергетических систем, утвержденных постановлением Правительства Российской Федерации от 13 августа 2018 г. № 937, п р и к а з ы в а ю:

1. Утвердить прилагаемые дополнительные требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы

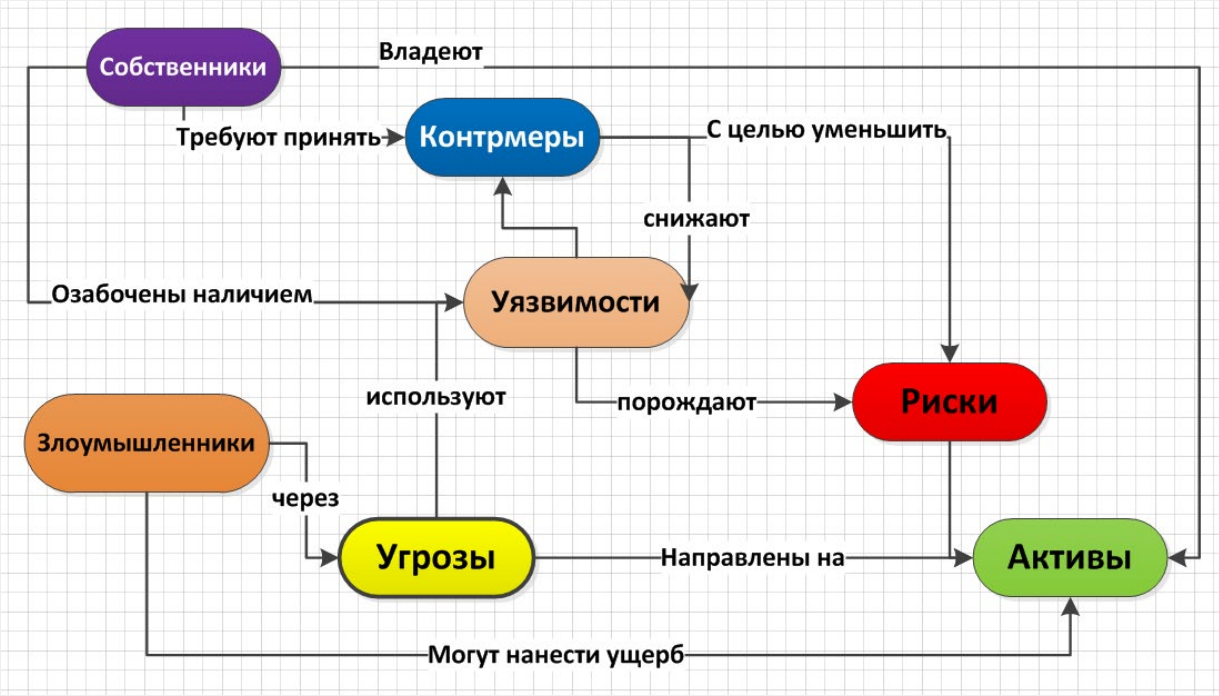
Пример: сервера точного времени vs средств РЭБ

- Средства радиоэлектронной борьбы подавляют, а наиболее продвинутые искажают сигналы систем глобального позиционирования.
- Места их развертывания и график включения в работу по понятным причинам не доводится до гражданских организаций.
- Этот же сигнал используют сервера точного времени.
- Синхронизация времени критически важна для правильной работы систем релейной защиты, векторных измерений (СВИ) координации работы устройств автоматизации и т. п.
- Это наглядная иллюстрация ситуации, когда десятилетиями развивающееся решение и достигшее технического совершенства, оказывается непригодным в условиях меняющейся реальности.

Типичные ошибки при планировании ИБ

- Неправильная оценка текущего состояния
- Ошибки в распределении ресурсов
  Безопасность комплексное понятие помимо ИБ туда входит, как минимум, физическая защищенность пожарная безопасность и т.п.
- Непропорциональный выбор решений
  ИБ – это тоже бизнес и маркетинговые компании игроков могут быть очень убедительны. Избыточные решения могут даже увеличить «поверхность для атаки»
- Пренебрежение простыми инструментами, например, организационного плана
- Просчеты в учете «человеческого фактора»
- Нерегулярный пересмотр мер защиты

Концептуальная модель информационной безопасности



Как их избежать?

- Развитие и обучение собственной команды
  Часть профильных специалистов должны освоить функцию ИБ, как дополнительную компетенцию
- Привлечение консультантов
- Использование передового опыта, в том числе зарубежного
  Лучшие практики хорошо документированы, есть в открытом доступе, например, в рабочих группах CIGRE
- Обмен опытом со смежными компаниями в отрасли, научной школой
- Взаимодействие с ГосСОПКА, даже если вы не объект, для которого это обязательно
- Принятие решений, основанных на объективных и актуальных данных и фактах
  С опорой на современные достижения статистики, аналитики технологий искусственного интеллекта и обработка данных

Стандарты и мировой опыт

- **NERC-CIP** (США и Азия);
- **BDEW White Paper** (Германия, Европа);
- **ISA-62443 (International Society of Automation)**
- **NIST Special Publications 800 series** (США);
- **ISO 27000 series** (международные)
- **Ausgrid** (корпоративный, Австралия)
- **CIGRE**

Это только источники! Каждый источник содержит десятки, иногда сотни документов.

Разумно не доверять устройствам и ПО, но специально плохих стандартов не напишут :)

Классификация тактик злоумышленников

v15.1

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques

1. Разведка (10)
2. Подготовка инструментов и ресурсов (8)
3. Первоначальный доступ (10)
4. Исполнение (14) – , атака, взлом, запуск вредоносного кода
5. Обеспечение постоянного присутствия (20)
6. Эскалация привилегий (14)
7. Избежание обнаружения (43)

- Доступ к учетным данным (17)
- Поиск и сбор данных (32)
- Миграция (9) - расширения контроля и доступа
- Сбор конфиденциальных данных (17)
- **Управление и контроль (18)**
- Вывод данных (9)
- Воздействие (14) - продажа или уничтожение данных

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques

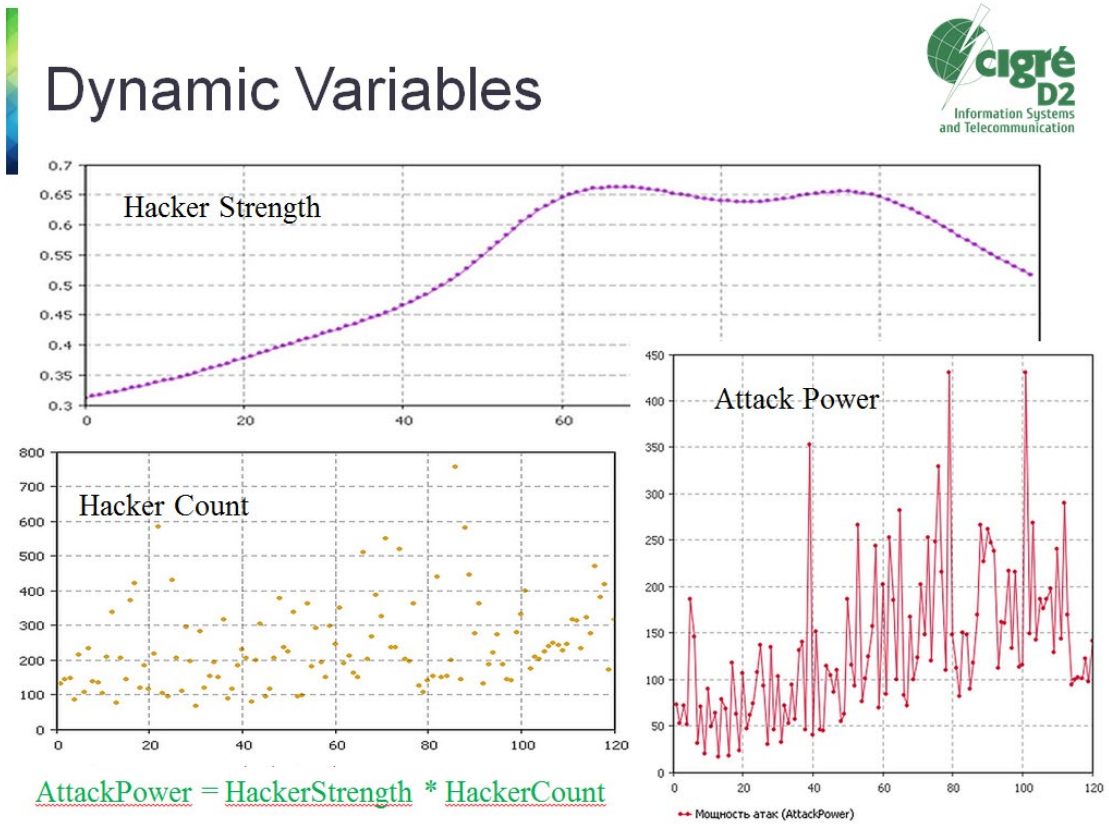
Common Vulnerability Scoring System (CVSS)

CVSS v.4.0 является развитием CVSS v.3.1

Опубликован в конце 2023 г.

Имитационное моделирование

- Имитационное моделирование новый быстроразвивающийся тренд, который позволяет строить модели на стыке разных дисциплин. Например, экономики, ИБ и технологии.
- **ИТ инфраструктура и ее защищенность успешно описывается графами**
- Многофакторный анализ сложная задача, но математический аппарат, хорошо разработанный для других областей, пока мало используется в ИБ
- И специалистам и лицам, принимающим решения остро не хватает наглядной визуализации и простых метрик.



В 2017 г. была построена имитационная модель с целью долгосрочного прогнозирования количества уязвимостей в отрасли с ростом киберугроз.

Модели могут стать одним из факторов, снижающих нагрузку на специалистов по ИБ, и позволяющие получить объективную картину путем расчета большого количества сценариев

Новая парадигма обеспечения надежности и => ИБ

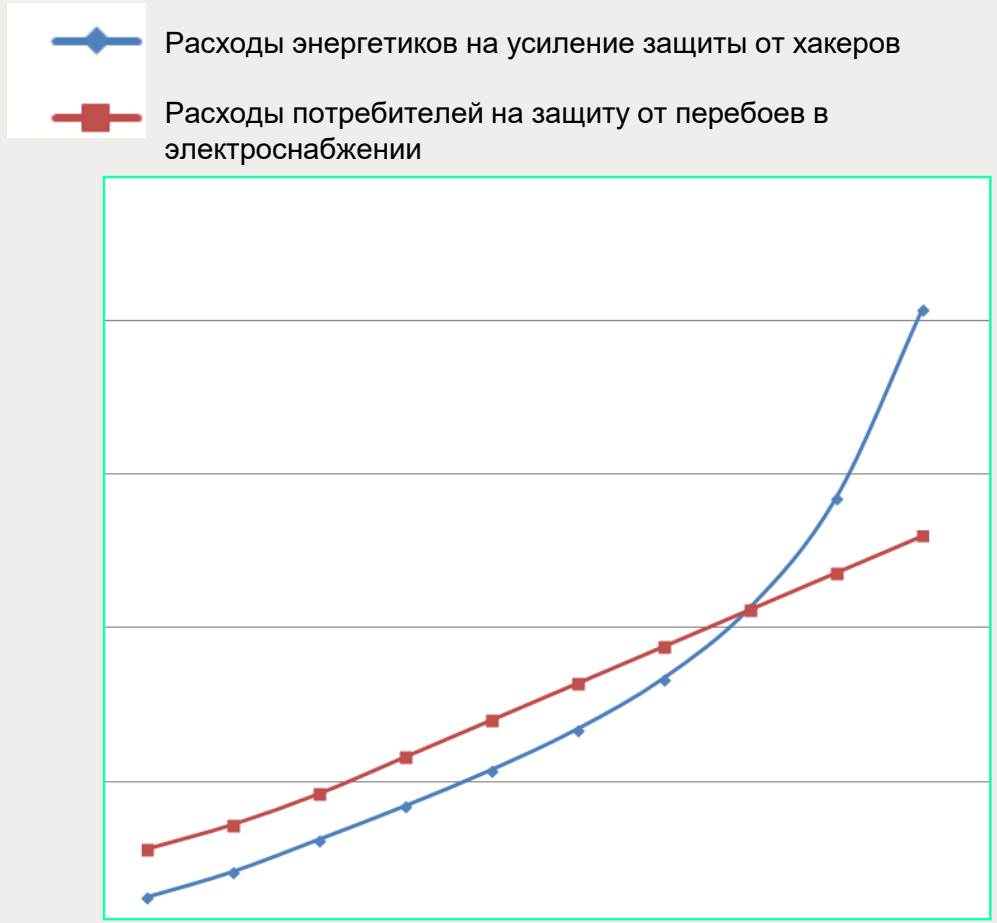
- ✓ Переход к управлению надежностью с оптимизацией совокупных расходов энергетиков и потребителей на обеспечение надежности (экономические стимулы)
- ✓ Потребители принимают максимально активное участие в управлении нагрузкой, локальной генерации и резервировании
  (концепция интернета энергии или ЭНЕРНЕТ)
- ✓ Современные достижения в области информационных и телекоммуникационных технологий становятся фундаментом интеллектуальных электрических сетей (ИЭС).
  (прикладной уровень – набор технологий smart grid)
- ✓ Государственная политика, закрепленная в программе «Цифровая экономика РФ» (и новая регуляторная база)

Эффект от перехода к управлению безопасностью

Риск = Вероятность (энергетики) * Ущерб (потребитель)

- Задача энергетиков **уменьшить вероятность** перебоев в электроснабжении
  Потребитель в свою очередь, должен принимать меры к **минимизации ущерба** от перерывов в электроснабжении.

- Это экономически целесообразно:
  - **100% защита от взлома недостижима!**
  - расходы на достижение и поддержание более высоких уровней информационной защищенности растут быстро и нелинейно (иногда экспоненциально!)
  - убытки от перерывов в электроснабжении, если предотвратить катастрофические последствия, линейно пропорциональны времени



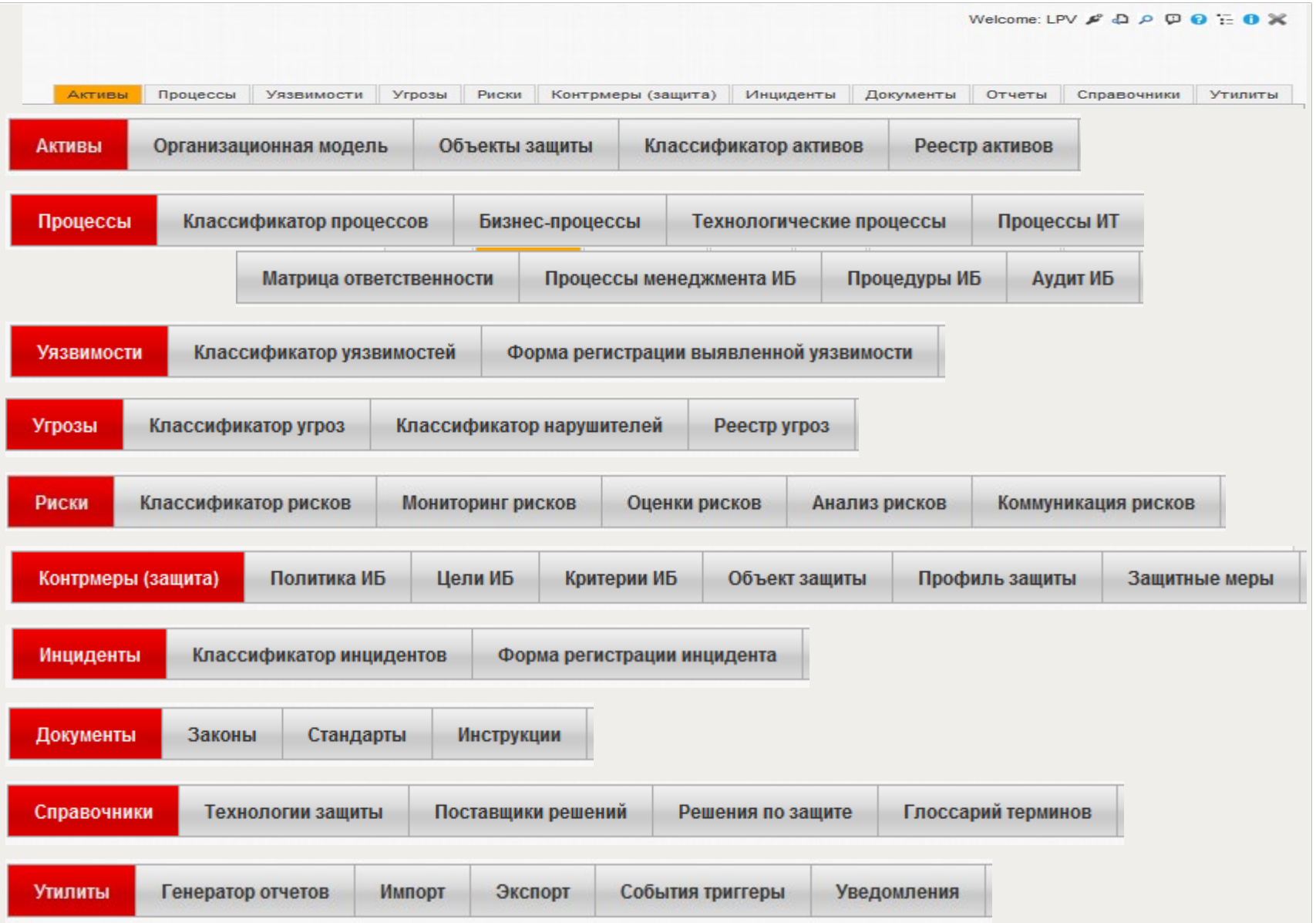
Верно в случаях если не было повреждения первичного оборудования!

Эталонная модель процесса (ЭМП) для управления информационной безопасностью

- Поднять эффективность управления можно декомпозировав его на процессы
- ГОСТ 57640-2017 идентичен международному ISO/IEC TS 33052:2016
- 69 стр. очень конкретных рекомендаций в структуре:
  - название
  - цель
  - контекст
  - выходные результаты
  - прослеживаемость требований

Специализированные информационные системы. Где они?

- Область сложна и очевидна потребность в ИС для планирования, документооборота, отчетности и т.п.!
- У бухгалтерии 1С, юристов – Гарант, отдел сбыта – CRM, производство – ERP.
- С чем работают Ваши «безопасники»?!



Так могло бы выглядеть меню специализированной информационной системы, «Моделирования и поддержки жизненного цикла решений по обеспечению безопасности»

Практические рекомендации

Изолировать не критичные для бизнеса решения
Если ваш сайт находится в той же зоне, что и производственные, перенесите его на хостинг;
Уменьшить поверхность для атаки
Пересмотрите все унаследованные решения, которые мало используются и откажитесь от них;
Задуматься над политикой «нулевого интернета» в корпоративной сети
Ваши сотрудники все что им надо для общения и для работы смогут получить на своих смартфонах, планшетах, ноутбуках, не подключенных к корпоративной сети.
Пересмотреть политику резервирования. Убедиться, что можно «подняться» из Backup
Зачастую критичные для бизнеса файлы можно уместить на «бытовом» NAS;
Остерегаться субподрядчиков
Если взломают, компанию, которая поставляет вам воду для кулера, а это сделать легко они не объект КИИ, то при наличии излишнего доверия «инфекция» может проникнуть и ваши ИС;
Вести журналы и логи событий, защищать их от изменений
Без них ни ваши сотрудники ни эксперты не смогут провести расследование атак и уязвимостей;
Не увлекаться борьбой с APT угрозами
Как показывает практика, чаще всего проблемы возникают из-за элементарных просчетов и ошибок
Убрать из публичного доступа информацию об инфраструктуре и способах ее защиты
Зачастую в старой конкурсной документации можно найти и хакерам уже не требуется «разведка»
Использовать решения и опыт коллег из спецслужб и смежных областей
(Пример с каналами связи и организацией обмена данными в иерархических системах)

Спасибо за внимание

litvpv@yandex.ru

cigre
For power system expertise