Российский национальный комитет Международного Совета
по большим электрическим системам высокого напряжения

ФГБОУ ВПО «Ивановский государственный энергетический
университет имени В.И. Ленина»

# ПИСЬМЕННЫЙ ПЕРЕВОД

научно-технического текста для участия в конкурсе переводчиков
научно-технической литературы Молодежной секции РНК СИГРЭ

Выполнили:
Брындин А.А.
Выборнова Е.А.
Новиков А.А. – стр.1-64
Демидов Ю.И.
Харчевников Н.М.
Хохлова А.Е. – стр.64-121
Редактор:
Выборнова Е.А.

Иваново 2016

603

# Организация и проведение мероприятий по информационной безопасности систем защиты и управления

## Объединенная Рабочая Группа B5/D2.46

Декабрь 2014

# ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМ ЗАЩИТЫ И УПРАВЛЕНИЯ

## Объединённая Рабочая Группа B5-D2.46


**Участники**

Деннис К. ХОЛСТЕЙН (США) Руководитель, Т.В. КЕАС (США) Секретарь/Издатель, Чарльз НЬЮТОН (США), Джейн СТАРК (Финляндия), Йошузуми СЕРИЗАВА (Япония), Шигеки КАТАЯМА (Япония), Йохан МАРИК (Бельгия), Андре СУХР (Германия), Йорг ЛАЛИНД (Испания), Джаквис САУВ (Бразилия), Ханнес ХОЛМ (Швеция), Майк СИВОЛЬД (Германия), Горан ЛЕЦИ (Хорватия), Жан-Мари БУАССЕ (Франция), Пауло ПЕРЕЙРА (Португалия), Стефан ТОМСОН (Соединенное Королевство Великобритании и Северной Ирландии) Автор, Родни ХАГЕС (Австралия), Тендай ЧАДИЯ (Австралия), Майкл ФОТОШ (Канада), Жорд МЕНДЕС (Португалия), Жан-Люк РОБИЧАУД (Канада), Питер РИТМАН (Швейцария); Санджив Коул (Индия), Убиратан Алвес ду КАРМО (Бразилия), Джозеф ВЕЙС (США), Ральф МАЦКЕВИЧ (США), Скот Д. СТРЕНФИЛД (США), Алекс ВОНГ (США), Крис ХАНТЛИ (Канада), Кейс СТАУФФЕР (США), Джон БЕНКЕНШТЕЙН (США),Ральф ЛАНГЕР (Германия), Людовик ПЬЕТРЕ-КАМБАСЕДЕС (Франция), Йенс ЗЕРБСТ (Швеция), Джон МАКДОНАЛЬД (Франция); Майкл СКОТТ (Австралия), Кристоф Пурьер (Франция)





ISBN : 978-2-85873-304-0

# Организация и проведение мероприятий по информационной безопасности для систем защиты и управления

## Оглавление


1 Предметная область брошюры ..... 8
2 Введение и основные принципы данной работы ..... 8
**2.1 Система защиты и управления – Что подразумевается под защитой и управлением** ..... 8
**2.2 Теоретическая структура** ..... 9
2.2.1 Развитие необходимых навыков при взаимодействии различных служб ..... 11
2.2.2 Сегодня, завтра и послезавтра ..... 12
**2.3 Влияние стандартов МЭК 62351 и МЭК 62443 на проведение дополнительных испытаний** ..... 14
3 Краткие выводы и рекомендации ..... 14
**3.1 Кибератаки и способы противодействия для систем защиты и контроля** ..... 14
**3.2 Рекомендации для практических решений в системе защиты и управления** ..... 16
**3.3 Десять основных замечаний** ..... 17
4 Угрозы информационной безопасности систем защиты и управления ..... 18
**4.1 Введение в проблему угроз информационной безопасности** ..... 18
**4.2 Реальные угрозы системам защиты и управления** ..... 18
4.2.1 Введение в проблему реальных угроз системам защиты и управления ..... 18
4.2.2 Уязвимости, возникавшие в ходе развития ..... 19
4.2.3 Уязвимости, возникающие на этапе внедрения и технической эксплуатации ..... 20
**4.3 Карта угроз и отбор наиболее вероятных угроз** ..... 23
**4.4 Предоставляют ли сигналы, передаваемые знаменитой системой GOOSE, возможности для совершения кибератаки против системы защиты и управления** ..... 26
4.4.1 Применение системы GOOSE для защиты ..... 26
4.4.2 Маршрутизированный GOOSE и выборочные значения для передачи информации устройств синхронизированных векторных измерений ..... 26
**4.5 Уязвимости в неподключенных и защищенных системах** ..... 27
4.5.1 Введение ..... 27
4.5.2 Миф о физической изоляции системы защиты и управления ..... 27
4.5.3 Неподключенные системы ..... 28
4.5.4 Уязвимости доверенных систем ..... 29
**4.6 Вынесенные уроки после нападения вирусам Stuxnet** ..... 31
4.6.1 Введение ..... 31
4.6.2 Опытные злоумышленники нацелены не на IT системы, а на системы управления ..... 31
4.6.3 Легкий способ преодоления физической изоляции ..... 32
4.6.4 Проверки целостности данных недостаточно ..... 33
**4.7 Последствия угроз для систем защиты и управления и систем SIPS** ..... 33
5 Каковы практические решения для реализации информационной безопасности в системах защиты и управления ..... 33

6 Практические примеры нормальной работы системы для оценки влияния на систему информационной безопасности ..... 34
**6.1 Исходные параметры системы защиты и управления, необходимые при определении и анализе виртуальных инцидентов** ..... 34
6.1.1 Стратегия реагирования инженеров по эксплуатации систем защиты и управления на появление виртуальных угроз ..... 34
6.1.2 Реакция на неисправность в режиме реального времени ..... 34
6.1.3 Оценка инцидентов в системе информационной безопасности ..... 36
6.1.4 Необходимость надлежащей подготовки инженеров системы защиты и управления по вопросам информационной безопасности ..... 36
6.1.5 Важные исправления компонентов в системе защиты и управления ..... 37
**6.2 Использование переносных носителей техническим персоналом – см. наглядный пример в Приложении L** ..... 38
6.2.1 Введение ..... 38
6.2.2 Необходимые функции обеспечения безопасности на мобильных устройствах ..... 39
6.2.3 Инструмент для анализа вариантов смягчения последствий ..... 40
**6.3 Управление на лицевой панели** ..... 41
6.3.1 Настройка управления на лицевой панели ..... 41
6.3.2 Тестирование вводов на лицевой панели ..... 42
**6.4 Управление безопасностью HMI** ..... 42
6.4.1 Введение в управление безопасностью HMI ..... 42
6.4.2 Предотвращение появления вредоносных программ ..... 42
6.4.3 Идентификация и опознавание ..... 43
6.4.4 Безопасность и административная конфигурация ..... 44
**6.5 Обеспечение соблюдения организационной и управленческой политики в области информационной безопасности** ..... 44
6.5.1 Изменения исполнительных нормативов ..... 45
6.5.2 Доступ сторонних организаций к цифровой системе автоматизации подстанции ..... 45
6.5.3 Обслуживающий персонал ..... 45
Приложение A Определение терминов и сокращений ..... 46
A.1 Определения терминов ..... 46
A.2 Используемые сокращения ..... 52
Приложение B Список литературы ..... 56
Приложение C Примеры электрических систем под воздействием кибератак ..... 59
Приложение D Обзор действующих отчетов, стандартов и передовых практических методов ..... 63
D.1 Технический подход, который использовался для обзора публикаций в отрытом доступе и проведения оценок ..... 63
D.2 Результаты опроса о защите и управлении ..... 65
D.2.3.1 Введение ..... 71
D.2.3.2 Получают ли инженеры, эксплуатирующие системы защиты и управления, необходимую начальную подготовку для обнаружения информационных атак ..... 71
D.2.3.3 Располагают ли инженеры систем защиты и управления необходимыми инструментами для борьбы с информационными атаками? ..... 72
D.2.3.4 В достаточной ли мере инженеры систем защиты и управления проверяют исправления, вносимые в системы? ..... 73
D.2.3.5 Какие решения необходимы по мнению инженеров систем защиты и управления ..... 73
D.2.3.6 В чём заключаются ограничения по использованию персональных электронных устройств для технического обслуживания или настройки элементов

систем защиты и управления? ..... 73
D.2.3.7 Как требования нормативных документов влияют на эксплуатацию систем защиты и управления? ..... 74
D.2.3.8 Выводы, полученные из анализа результатов исследования ..... 74
Приложение E Безопасная адаптация персональных устройств к системам защиты и управления и их составляющим ..... 76
E.1 Будущее близко ..... 76
E.2 Риски, которыми необходимо управлять ..... 76
E.3 Безопасное сопряжение персональных устройств ..... 76
Приложение F Обеспечение безопасности систем защиты и управления от атак межсайтового скриптинга ..... 78
F.1 Межоперационные системы защиты и управления уязвимы перед атаками межсайтового скриптинга (XSS, Cross-Site Scripting) ..... 78
F.2 Предотвращение XSS требует участия всех заинтересованных сторон ..... 80
Приложение G Криптографические функции хэширования ..... 83
G.1 Функции хэширования используются для обеспечения безопасности релейной защиты и управления ..... 83
G.2 Основные приложения системы защиты и управления, использующие функции хэширования ..... 83
G.3 Нужно иметь в виду новые проблемы функций хэширования ..... 84
Приложение H Предотвращение атак переполнения стека ..... 85
H.1 Введение ..... 85
H.2 Что происходит в случае переполнения стека и почему это опасно ..... 85
H.3 Каким образом нарушитель пользуется схемой ..... 86
H.4 Хорошая новость - плохая новость ..... 87
Приложение I Системам защиты и управления необходимо программное обеспечение, гарантирующее масштабируемую защиту на всех уровнях ..... 88
I.1 Вступление ..... 88
I.2 Идти в ногу со временем ..... 88
I.3 Диапазон настраиваемой надежности ..... 89
I.4 Метод «плавающей точки» для обеспечения устойчивости посредством «увеличенной скорости» ..... 89
Приложение J Участие инженеров релейной защиты и управления в аудите конфигурации ..... 91
J.1 Необходимость аудита конфигурации систем защиты и управления ..... 91
J.2 Важность автоматизации ..... 91
J.3 Аудит против управления ..... 92
Приложение K Своевременное выявление возможных угроз ..... 94
K.1 Сокращение времени отклика защиты требует своевременного распознавания угрозы ..... 94
K.2 Структура системы разрешения проблем безопасности ..... 94
K.3 Онтологии, используемые для организации данных, используемых для обработки инициированной кибератаки ..... 94
K.4 Систематизация кибератак на основе последствий ..... 95
Приложение L Модель оценки CySeMoL ..... 98
L.1 Введение в CySeMoL ..... 98
L.2 Модели сети ..... 101
L.3 Сценарии кибератак ..... 105
Приложение M Жизненный цикл управления ключами ..... 108
M.1 Введение в управление ключами ..... 108
M.2 Формы ключей ..... 108
M.3 Жизненный цикл использования ключевого материала ..... 108

M.4 Требования ПСАУ, влияющие на схемы управления ключами ..... 110
M.4.6.4 Запрос о комментариях (RFC) 3647 ..... 114
M.5 Работа ПСАУ требует эластичное управление ключами ..... 114
Приложение N Опасные последствия в системах защиты и управления и схемах защиты целостности системы (SIPS) ..... 116
N.1 Вступление ..... 116
N.2 Предположение успешной атаки на цифровую релейную защиту ..... 118
N.3 Угроза защитам линии и ее влияние на энергосистему ..... 119
N. 4 Угрозы системам SIPS ..... 122
N. 5 Общесистемные SIPS - наиболее сложные системы ..... 123
Приложение O Детальное рассмотрение практических решений информационной безопасности ..... 128
O.1 Совместные усилия ..... 128
O.2 Физическая защита систем защиты и управления ..... 128
O.3 Безопасность оконечного устройства систем защиты и управления ..... 128
O.4 Контроль сетевой безопасности систем защиты и управления ..... 129
O.5 Эксплуатационные ограничения ..... 134
O.6 Максимальное использование компенсирующих механизмов безопасности ..... 135
Приложение P Расширение рекомендаций США по укреплению защиты информационной безопасности ..... 139
P.1 Отчет Комитета советников при Президенте США по вопросам науки и техники (PCAST) ..... 139
P.2 Основной вывод ..... 139

## Список иллюстраций

Рисунок 1 Теоретическая структура, используемая в данной брошюре ..... 10
Рисунок 2 Реакция инженеров по эксплуатации системы защиты и управления на виртуальную неисправность ..... 35
Рисунок 3 Срочное исправление компонентов в системе защиты и управления ..... 37
Рисунок C-4 Пример системы напряжением 735 кВ ..... 59
Рисунок C-5 Влияние отключения, вызванного кибератакой ..... 60
Рисунок C-6 Регулирование сети путем уменьшения реактивной мощности ..... 60
Рисунок C-7 Результаты ослабленной системы ..... 61
Рисунок C-8 Влияние на систему в случае потери всей компенсации ..... 62
Рисунок C-9 Потеря поперечной компенсации ..... 62
Рисунок D-10 Распределение голосов опрашиваемых компаний ..... 66
Рисунок E-11 BYOD - планшет ..... 76
Рисунок H-12 Строение стека (опубликовано в [57]) ..... 85
Рисунок H-13 Переполнение стека (опубликовано в [57]) ..... 86
Рисунок H-14 Атака переполнения стека (опубликовано в [57]) ..... 87
Рисунок K-15 Возможная схема системы разрешения проблем безопасности ..... 95
Рисунок K-16 Взаимодействие с угрозой ..... 96
Рисунок L-17 Общее описание объектов CySeMoL и их связи ..... 99
Рисунок L-18 Общая схема модели сети ..... 102
Рисунок L-19 Общая схема удаленного доступа к оборудованию системы защиты и управления из внутренней сети ..... 103
Рисунок L-20 Роли персонала системы защиты и управления, учетные записи и программные средства ..... 104
Рисунок L-21 Описание программного обеспечения в сети системы защиты и управления ..... 104
Рисунок M-22 Цикл управления ключами ..... 109
Рисунок N-23 Основная иерархическая структура систем SIPS, RAS или SPS ..... 117
Рисунок N-24 Типовые кривые зависимости напряжения от мощности ..... 119

Рисунок N-25 Кривая нагрузки на графике зависимости напряжения от мощности ..... 120
Рисунок N-26 Равновесная точка на графике зависимости напряжения от мощности ..... 121
Рисунок N-27 Влияние, вызванное потерей компенсации ..... 122
Рисунок N-28 Функциональная структура и пути обмена информацией систем с широкой зоной контроля ..... 124
Рисунок O-29 802.1x Контроль доступа ..... 132
Рисунок O-30 Процесс управления уязвимостями ..... 136

## Список таблиц

Таблица 1 Кибератаки и способы противодействия ..... 15
Таблица 2 Карта угроз системы защиты и управления ..... 25
Таблица 3 Вероятность успеха кибератаки через USB-порт ..... 41
Таблица 4 Руководящие принципы контроля безопасности против появления вредоносных программ ..... 43
Таблица 5 Руководящие принципы по управлению административной безопасностью ..... 44
Таблица D-6 Отчеты по вопросам информационной безопасности систем защиты и управления ..... 63
Таблица D-7 Стандарты для защиты информационной безопасности систем защиты и управления ..... 63
Таблица D-8 Рекомендации по информационной безопасности систем защиты и управления ..... 65
Таблица D-9 Вопросы для исследования информационной безопасности систем защиты и управления ..... 66
Таблица F-10 Степень участия в обеспечении безопасности систем защиты и управления при атаках межсайтового скриптинга ..... 81
Таблица L-11 Краткое описание категорий CySeMoL ..... 100
Таблица N-12 Эксплуатационные и коммуникационные требования к системам WAMPAC ..... 125
Таблица N-13 Влияние кибератак на надежность и эксплуатационные требования, их последствия и контрмеры (примеры) ..... 126

# 1 Предметная область брошюры

Исследовательскому комитету (ИК) CIGRE B5 было поручено провести данное исследование в сентябре 2011 года для того, чтобы лучше разобраться в задачах по организации и проведению мероприятий в сфере информационной безопасности[1], возлагаемых на организации, эксплуатирующие системы защиты и управления. Основной проблемой рабочей группы является описание этих задач на языке, понятном для инженеров систем защиты и управления.

Поскольку задачи организации и проведения мероприятий по информационной безопасности систем защиты и управления в основном взяты из основ информационных технологий, в феврале 2012 г. CIGRE решил создать совместную рабочую группу с ИК D2. В связи с этим ИК B5 был преобразован и 1 марта 2012 г. было утверждено техническое задание.

Для выявления основных принципов этого исследования, сразу после краткого введения во 2 пункте, в 3 пункте формулируется основные выводы. В 4 пункте описываются общие сведения об угрозах информационной безопасности для систем защиты и управления. В 5 пункте предлагается краткий список практических решений для обеспечения информационной безопасности. Наконец, в 6 пункте содержатся реальные примеры информационных атак на системы защиты и управления. В дополнение к определению терминов и аббревиатур, в работе даётся подробный библиографический список источников. В приложениях обращается особое внимание на (Приложения позволяют глубже погрузится в) основные вопросы безопасности. В добавлении к библиографическому списку, в приложении D содержатся действующие стандарты, отчёты и эксплуатационные рекомендации, касающиеся возможных угроз для систем защиты и управления.

# 2 Введение и основные принципы данной работы

## 2.1 Система защиты и управления – Что подразумевается под защитой и управлением

Для сохранения устойчивой работы ЭЭС и обеспечения надёжного снабжения электроэнергией своих потребителей электроэнергетическая компания должна выполнять широкий спектр задач, связанных с защитой и управлением. В рамках данной технической брошюры практически невозможно затронуть все возможные вопросы, связанные с организацией и проведением мероприятий в области информационной безопасности. В будущем рабочие группы затронут вопросы внедрения и организации механизмов информационной защиты для систем контроля и сбора данных (SCADA) и для устройств управления работой энергосистем.

Данная техническая брошюра затрагивает те средства информационной безопасности, которые используются для ограничения доступа к системам защиты ЭЭС, в схемах противоаварийной автоматики (ПА), а также в локальных устройствах автоматики и управления подстанций. Инженер системы защиты и управления должен обеспечить удалённый доступ и использовать средства контроля за оборудованием систем защиты и управления и сетевыми устройствами. Кроме того, инженеру систем защиты и управления необходимо обеспечить средства защиты местного доступа к этим устройствам через локальную сеть подстанции или коммуникационный порт отдельного устройства.

В данном исследовании рассматриваются современные системы защиты и управления, соединённые высокоскоростными коммуникационными сетями, а также способы доступа к сетевым устройствам (таким как маршрутизатор и сетевой коммутатор) и вопросы их использования.

Целевую аудиторию данной технической брошюры составляют инженеры, технический персонал и начальники служб защиты и управления. Они имеют представление о технических средствах контроля за безопасностью доступа к системам защиты и управления и за их использованием. Учитывая степень подготовленности аудитории, необходимо описать технические средства

[1] Термин «информационная безопасность», использующийся в данной технической брошюре, позволяет избежать путаницы с термином «безопасность», который, в промышленном контексте, может иметь и другие значения, не связанные с информационной безопасностью систем защиты и управления (например, безопасность активов или физических лиц).

контроля информационной безопасности на понятном ей языке.

Определение некоторых качественных показателей позволяет судить о правильности решений в области информационной безопасности. Такая оценка необходима для решения трёх управленческих задач: (1) контроль происшествий, (2) контроль за наиболее уязвимыми местами, улучшениями, конфигурацией и изменениями и (3) контроль за безопасностью программных приложений.

Не менее важным является качество технических средств контроля информационной безопасности, которое определяет степень доверия сотрудников энергетических компаний и персонала технической поддержки к системам защиты и контроля. Также важно раскрыть основные допущения при управлении техническими средствами контроля.

### 2.2 Теоретическая структура

Теоретическая структура (информационной безопасности) должна обеспечивать целостный и всесторонний подход в отношении информационной безопасности. Понимание структуры информационной безопасности необходимо для правильного расположения технических средств контроля безопасности, также это способствует и общему пониманию работы ЭЭС. Довольно распространена практика, когда структура информационной безопасности дополняет общую функциональную структуру системы.

Для данной технической брошюры подходящим источником определений и терминов является терминологическая база подразделения МЭК ТС 57. Две рабочие группы WG 19 и WG 10 (МЭК 61850) из подразделения МЭК ТС 57 обозначили следующий системный подход. В 5 части стандарта МЭК 61850 содержатся определения, связанные с системой автоматизации подстанций. Эти определения охватывают полевой уровень (уровень процесса), уровень присоединений и станционный уровень подстанции, а также три основных вида внешних связей подстанции,

- Связь с другой подстанцией (дистанционная защита, обмен управляющими сигналами между подстанциями).
- Связь с центром управления (обмен управляющими сигналами между подстанцией и центром управления).
- Дистанционное управление: обмен данными между подстанцией (уровнем подстанции) и удалённым рабочим местом инженера.

Такой подход позволяет учитывать распределённую систему управления и функционал защиты. Кроме того, существует возможность размещения новых схем защиты на подстанции(ях) и в центре(ах) управления. Согласно системному подходу технического комитета ТС57, структура информационной безопасности, изображённая на рисунке 1, охватывает четыре основных случая использования систем защиты и управления.

1) Система автоматизации подстанции
2) Связь подстанции с другой подстанцией
3) Связь подстанции с центром управления
4) Дистанционное управление

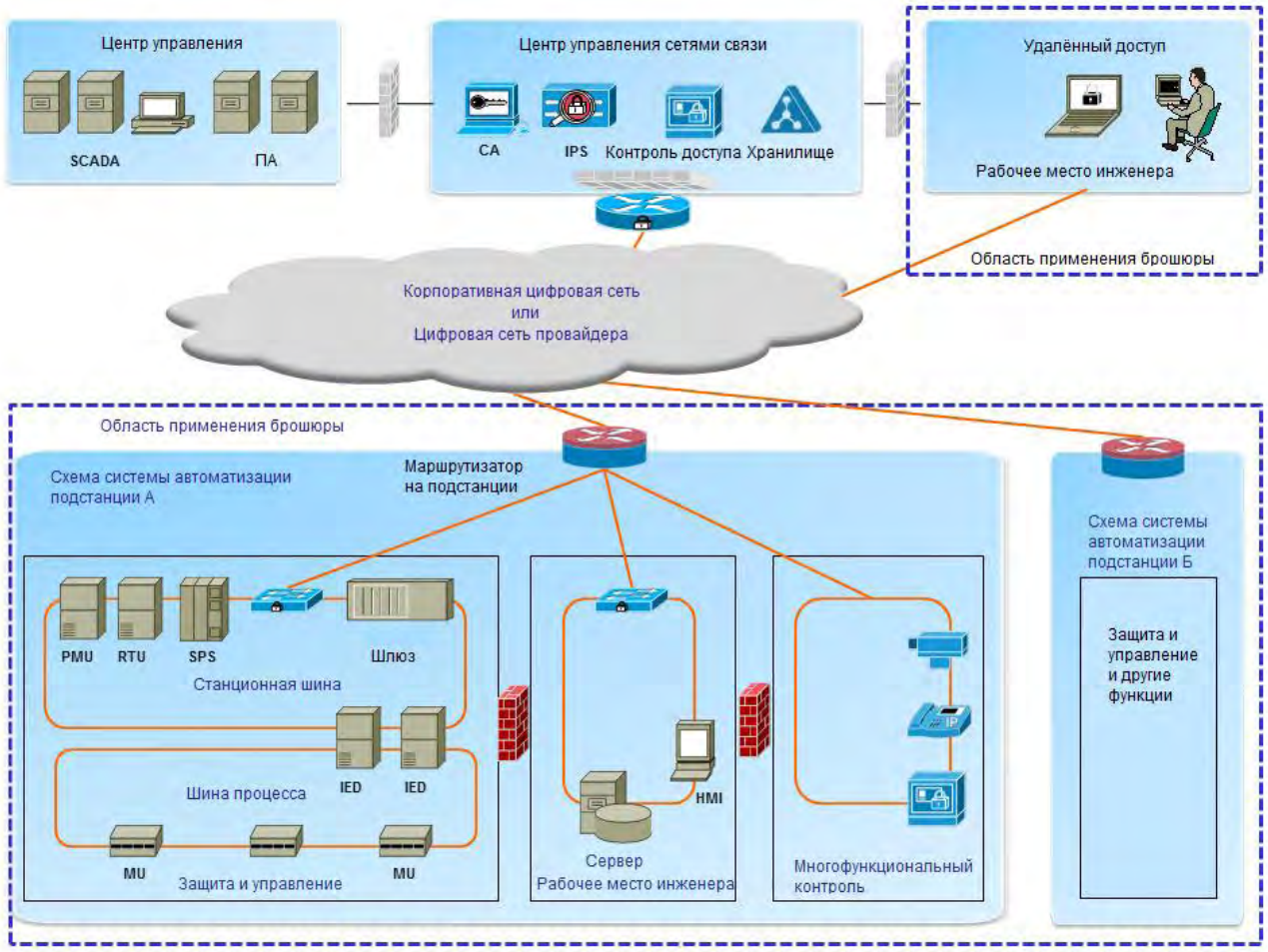



**Рисунок 1 Теоретическая структура, используемая в данной брошюре**

Главным компонентом данной структуры (и областью действия брошюры) является подстанция, которая содержит автоматизированную систему управления. Отдельные сегменты системы разделены логически. Сегментация допускает разделение трафика по виду устройств (например, устройства SCADA, управления) и может быть выполнена с использованием виртуальных локальных сетей. Кроме того, брандмауэры с зональной конфигурацией обеспечивают надёжную защиту периметра. На рисунке 1 автоматизированная система управления подстанцией состоит из трёх сегментов/зон.

1) Системы защиты и управления, в соответствии с рекомендациями МЭК 61850 подразделяется на станционную шину и шину процесса.

2) Рабочее место инженера

3) Многофункциональный контроль

Возможности сетевых устройств (коммутационных устройств, маршрутизаторов, брандмауэров) обеспечивают гибкость и способность к расширению при усовершенствовании структуры информационной безопасности. При необходимости в структуру могут быть добавлены дополнительные сегменты/зоны с новым функционалом и принципами работы.

### 2.2.1 Развитие необходимых навыков при взаимодействии различных служб

В прошлом проекты подстанций подразумевали использование схем защиты и управления, в основе которых лежали устройства, отвечающие за одну конкретную функцию; в большинстве случаев использовались схемы с жёсткой логикой. Однако спустя десятилетия, благодаря преимуществам использования многофункциональных интеллектуальных электронных устройств (ИЭУ), стали возможными повышение функциональности и, следовательно, сокращение количества данных устройств. В связи с массовым внедрением обмена цифровой информацией при помощи сетей связи и разработке таких стандартов, как МЭК 61850, в сфере защиты и управления стали возникать, помимо обыкновенных, и совершенно новые проблемы. Недостаток знаний о технологиях передачи данных, протоколах, удалённом доступе и угрозах, связанных с информационной безопасностью, способствует повышению вероятности возникновения происшествий в информационной среде. Инженерам систем защиты и управления требуется всё большее количество информации для решения множества проблем, связанных со средствами коммуникации и областью информационных технологий (ИТ).

В то же время, с появлением оптоволокна и высоких скоростей, возникших вместе с сетями передачи данных, стало возможным внедрение на подстанциях систем сбора данных, контроля и управления в реальном времени, что, в свою очередь, привело к появлению целого комплекса основных и вспомогательных служб. На объекте возможно существование нескольких локальных и глобальных сетей, которые так или иначе должны быть соединены между собой; соответственно, необходимо взаимодействие различных технических служб.

Хоть это и зависит от политики и стратегии каждой конкретной электроэнергетической компании, обычно сети, не относящиеся к системе защиты и управления, находятся в ведении либо IT персонала, либо персонала службы телекоммуникаций и исторически не принято создавать многопрофильные подразделения между этими отделами.

Некоторые сети имеют различные предназначения[2]. Кроме того, могут существовать значительные различия в плане мышления и технических навыков между IT-инженерами, инженерами телекоммуникаций и инженерами систем защиты и управления. С технической точки зрения, указанные сети и эксплуатирующие их службы очень близки и должны иметь много общих свойств, функциональных возможностей и проблем, а в некоторых случаях они должны быть взаимосвязаны.

Внедрение нового поколения технологий защиты и управления подстанций – это не только техническая, но и организационная задача. В самом деле, по мере того, как разрабатываются и применяются новые технические решения, очень важным становится вопрос привлечения инженеров систем защиты и управления, технического персонала и начальников служб к процессу развития и обновления, поскольку им потребуется некоторое время на обучение и понимание происходящего. Это необходимо для того, чтобы они могли уверенно обращаться с новыми технологиями, условиями и методами.

Недостаток знаний и отсутствие структурной взаимозаменяемости новых и старых технологий ставят перед инженерами систем защиты и управления важную задачу разработать и провести мероприятия по организации планирования, внедрения, эксплуатации и контроля за системами защиты и управления. Системы защиты и управления перестали быть только системами защиты и управления. Обычно, они подсоединяются к локальным сетям, которые, в свою очередь, подсоединяются к другим сетям передачи данных. Теперь инженеры защиты и управления должны обладать навыками в IT-сфере, чтобы соответствовать своей должности. По этой причине им важно понимать, что основные положения сетевых информационных технологий и информационной безопасности не так уж сложны. Им необходимо развивать общую лексику и взаимопонимание с IT-службами и службами телекоммуникаций, которые могут поделиться знаниями и способствовать коммуникативной интеграции.

IT-службы и службы телекоммуникаций электроэнергетических компаний должны, в свою очередь,

[2] Как правило, более крупные электроэнергетические компании имеют выделенные сети связи, в то время как более мелкие пользуются сетями общего пользования.

понимать особенности, нужды и проблемы процесса передачи информации между устройствами защиты и управления подстанций, который так важен для энергетической системы.

### 2.2.2 Сегодня, завтра и послезавтра

Последние несколько десятилетий новые технологии стремительно развивались и интегрировались в системы защиты и управления электроэнергетических компаний. Телекоммуникация, безусловно, находятся среди наиболее важных сфер, претерпевших изменения. Поскольку системы защиты и управления стали использовать системы телекоммуникации, первоочередной задачей и основным техническим требованием стали высокая эффективность и доступность информации.

На сегодняшний день, развитие телекоммуникаций в системах защиты и управления позволяет использовать более эффективные и гибкие технологии, такие как протокол DNP3-IP или стандарт МЭК 61850. Применение новых технологий приводит к возникновению новой задачи – обеспечение информационной безопасности. К её требованиям быстро адаптировались производители отдельных устройств, в основном это технические средства, связанные с ИТ и сетями (например, маршрутизаторы, брандмауэры и т.д.).

К сожалению, с системными устройствами защиты и управления, не обладающими сильной встроенной защитой от информационных атак, дело обстоит иначе. ИЭУ старого образца (а иногда даже и новые модели) часто не способны решать три важнейшие задачи обеспечения информационной безопасности (безопасный доступ, целостность и конфиденциальность данных).

Большинство стандартов и передовых методик обычно рекомендуют применять принципы «глубокоэшелонированной защиты». Чтобы обеспечить достаточное количество уровней защиты как для электронной защиты периметра, так и для конечного устройства, должны быть доступны несколько типов средств управления информационной безопасностью.

Для инженеров систем защиты и управления основной задачей сегодня является интегрирование средств управления системами информационной безопасности в уже существующую архитектуру эксплуатируемых систем. Фактически, это входит в их текущие обязанности. Инженеры должны регулярно осуществлять внедрение новых протоколов, устройств и технологий в системы защиты и управления. Аттестации и проверки являются частью их повседневной работы. Кроме того, существует очевидная необходимость относиться к вопросам применения и технического обслуживания средств управления системами информационной безопасности точно так же, как и к другим элементам систем защиты и управления. Инженеры систем защиты и управления должны действовать согласно стандартам и руководящим указаниям. Именно инженеры системы защиты и управления должны заставлять производителей соответствовать стандартам, таким как МЭК 62351, для того, чтобы упростить процесс интеграции средств контроля за информационной безопасностью в системы защиты и управления. В настоящее время стандарт МЭК 62351 состоит из девяти завершённых частей. Далее приведён список частей, содержащих детальное описание механизмов обеспечения безопасности, таких как защита транспортного уровня или криптография с симметричными шифрами для защиты протоколов, например, ICCP/TASE.2 или МЭК 61850: часть 3, 4, 5, 6, 8 и 10. Для того, чтобы сохранялась совместимость устройств, производители должны применять только определённые средства обеспечения безопасности. Как и в случае со стандартом МЭК 61850, после того, как достаточное количество производителей ИЭУ примут МЭК 62351, правила эксплуатации устройств, подсистем и систем станут содержать соответствующие требования по проверке на соответствие стандартам и сертификации. Кроме того, может быть учтена проверка совместимости оборудования, так как любые новые устройства должны корректно взаимодействовать с уже установленными в виду наличия большого количества производителей оборудования.

В обязанности руководства входит обеспечение как можно более высокого уровня зашиты их энергосетей от происшествий в информационной среде без чрезмерно большой траты денег на средства контроля за информационной безопасностью существующих систем защиты и управления. В добавок к этому, остаётся значительная проблема: как повысить уровень знаний и навыков инженеров систем защиты и управления в новой для них сфере деятельности? Конечно, изменения в теоретической сфере, вызванные внедрением новых технологий, не должны становиться сюрпризом для руководства. Обучение и ознакомление являются ключом к решению

этой задачи, но, в конечном счёте, ответственность за мотивирование к внедрению и использованию соответствующих элементов контроля за безопасностью возлагается на отдельных работников. Руководство должно определять методы, с помощью которых будут обеспечены эти меры безопасности, а также механизмы проверки и оценки их соответствия.

Вполне вероятно, что в ближайшем будущем могут возникнуть новые проблемы. Во-первых, новые архитектуры и протоколы, такие как шина процесса, система «горизонтального» обмена информацией между устройствами[3] (GOOSE) и протокол Sample Value (SV) из МЭК 61850 привнесут свою долю проблем, связанных с информационной безопасностью. С точки зрения архитектуры, интеграция возобновляемых источников энергии и всё большее объединение систем защиты и управления требует большего использования распределённой логики и управления.

В ближайшем будущем критерием для внедрения средств контроля за информационной безопасностью будет не техническое обоснование, а оценка рисков и стоимости оборудования. Важным показателем успеха будет уход от сложных структур управления безопасностью. Эффективное использование возможностей существующих сетей позволит избежать чрезмерных затрат.

Кроме того, современные сетевые технологии, такие как автоматическое развёртывание (zero-touch-deployment), удалённое обслуживание и контроль могут упростить работу инженеров системы защиты и управления. Средства контроля за информационной безопасностью, соответствующие требованиям, должны будут по умолчанию устанавливаться в ИЭУ (например, в спецификации IEEE-Std-1686) и в протоколы (например, по стандарту МЭК 62351). В дополнение к этому, в ближайшем будущем ИЭУ должны будут обладать необходимым набором средств контроля за информационной безопасностью, чтобы инженеры защиты могли соблюдать стандарты и требования передовых методик. Задача состоит в обеспечении этих методов контроля безопасности при наличии ограничивающих эксплуатационных требований систем защиты и управления.

Надёжная сетевая информационная защита должна поддерживать безопасность оконечной точки и уменьшать нагрузку на ИЭУ и связанные с ними системы защиты и управления. Ни одна мера информационной безопасности, затрагивающая ИЭУ, не должна препятствовать его доступности и прочим важным атрибутам качества, таким как производительность и надёжность. Главной целью этих мер всегда является защита основного оборудования для обеспечения стабильной работы электрической сети.

Сфера действия систем защиты и управления также выходит за пределы ‘традиционной’ связи и прикладных программных средств, поддерживающих только устройства защиты и управления. После создания локальной вычислительной сети (ЛВС) на подстанции новые программные приложения смогут дублировать управление сетевым оборудованием. Контроль состояния является типичным примером тех решений, разрабатывающихся в МЭК 61850-90-3[4], в котором для одного только контроля состояния трансформаторов предусмотрено около 18 типов датчиков. Аналогичным образом, ЛВС на территории подстанции вполне может понадобиться для работы телефонной связи и даже для физической защиты и наблюдения, к примеру, посредством видеокамер.

В настоящее время для ЛВС подстанций применяются кабели Cat5/Cat6 Ethernet или оптоволокно, что требует наличия физического соединения для подключения к ЛВС. Однако, как подчёркивается в технической брошюре СИГРЭ 318, опубликованной в 2007 году, устройства, подключаемые к Wi-Fi, расширяют ЛВС и увеличивают её доступность. Физическая среда передачи данных ЛВС подстанций также находится на грани существенного географического расширения под воздействием требований Smart Grid технологий.

Эти изменения поднимают планку эффективного контроля за информационной безопасностью.

[3] Сообщения GOOSE представляют собой многоадресные сообщения об изменении состояния. Через заранее определённые интервалы времени GOOSE-сообщение повторяется с целью повышения вероятности корректного приёма информации.
[4] МЭК 61850-90-3 “применение МЭК 61850 для контроля состояния” находится в разработке.

Помимо оконечной точки и сегодняшних возможностей сетевой информационной защиты, будут развиваться новые технологии, такие как информационная безопасность на основе анализа поведения[5].

### 2.3 Влияние стандартов МЭК 62351 и МЭК 62443 на проведение дополнительных испытаний

Прежде чем говорить о МЭК 62351и МЭК 62443, важно принять во внимание рекомендации Европейского агентства по сетевой и информационной безопасности ENISA. Согласно отчёту ENISA “Руководство по информационной безопасности интеллектуальных сетей для Европы и стран ЕС” [1], для интеллектуальных сетей следует рассматривать использование общих критериев (ИСО/МЭК 15408). Стандарт ИСО/ МЭК 15408 может служить инструментом для оценки степени защищённости систем, устройств и программ защиты и управления. Он определяет множество профилей защиты для оценки различных аспектов безопасности систем защиты и управления. Примерами существующих профилей защиты, которые могут быть полезными для систем защиты и управления являются *Системный контроль доступа, система интеллектуального учёта шлюза* и *профиль защиты операционных систем*.

Для электроэнергетических систем подразделение МЭК TC57 WG15 является ведущей организацией, вырабатывающей стандарты информационной безопасности. Для систем промышленной автоматизации таковой является подразделение МЭК TC65 WG10. Эти две организации поддерживают формальную связь друг с другом, чтобы обеспечить совместимость между стандартами МЭК 62351 (разработан TC57 WG15) и МЭК 62443 (разработан TC65 WG10). В данных стандартах каждая часть включает краткое описание сферы своего действия.

МЭК 62443 не ссылается непосредственно на МЭК 61850, тогда как МЭК 62351, часть 3, 4, 6, 7, 8 и 10, приводит подробные выдержки из МЭК 61850 [2]. МЭК 62351 не устанавливает конкретных требований к испытаниям информационной безопасности для МЭК 61850. МЭК 62443-2-4 [3] косвенно закладывает основу для тестирования систем по стандарту МЭК 61850. Однако, на момент публикации данной технической брошюры, МЭК 61850 не ссылается на требования к испытаниям информационной безопасности ни из стандартов МЭК 62351, ни из МЭК 62443.

Приложения к настоящей технической брошюре содержат комментарии к конкретным частям МЭК 62443. Ко времени публикации настоящей технической брошюры большинство частей стандарта 62443 находились в стадии разработки.

## 3 Краткие выводы и рекомендации

### 3.1 Кибератаки и способы противодействия для систем защиты и контроля

Данная техническая брошюра концентрирует внимание на различных типах кибератак, их возможных последствиях и на способах противодействия кибератакам, которые интересуют инженеров систем защиты и управления. Для правильного восприятия, обобщим основные вопросы не вдаваясь в подробности. На доступном языке в таблице 1 кибератаки разделяются на 4 категории. Атаки по сбору данных предполагают просмотр или повреждение (изменение) данных системы защиты и управления, подслушивание (прослушивание/запись связи между интеллектуальным электронным устройством (ИЭУ) системы защиты и управления и зарегистрированными пользователями) и выполнение анализа передвижения повторяющихся моделей общения между ИЭУ системы защиты и управления и зарегистрированными пользователями. Имитационные типы атак, такие как подмена, клонирование и повтор предполагают имперсонацию законного доступа к ИЭУ или между несколькими ИЭУ системы защиты и управления для получения несанкционированного доступа. Блокирующие атаки разрушают сетевые ресурсы системы защиты и управления, ИЭУ или мешают коммуникации, используя такие приемы, как отказ в обслуживании и сжатие вредоносных программ. Атаки на конфиденциальные данные стремятся разгласить конфиденциальную информацию о законных пользователях или группах системы защиты и управления. Кибератаки могут возникать

[5] Для обеспечения безопасности на основе анализа поведения требуются адаптивные самообучающиеся программы.

согласованно или независимо, что приводит к потере системой защиты и управления доступности, целостности и конфиденциальности данных.

**Таблица 1 Кибератаки и способы противодействия**

| Категории атак | Типы атак | Возможные последствия | Способы противодействия |
|---|---|---|---|
| Блокирующие | Отказ в обслуживании: переполнение потоков данных системы защиты и контроля, разрушающих системные или сетевые ресурсы системы защиты и управления, или мешающих ее коммуникации | Потеря доступности данных системы защиты и управления | Система сетевой защиты периметра, сетевой машрутизатор для контроля системы защиты и управления, ресурсоувеличение, распределенная динамическая фильтрация пакетов и контроль перегруженности |
| | Сжатие: электромагнитные помехи или запрет использования той же частоты-диапазона беспроводных сигналов | Потеря доступности данных системы защиты и управления | Анти-помехи, активные помехи, и клетки Фарадея.<br><br>Примечание: клетка Фарадея или щит Фарадея представляет собой корпус, образованный токопроводящим материалом или сеткой из такого материала. Такая оболочка блокирует внешние статические и нестатические электрические поля. |
| | Вредоносные программы: распространяющие вирусы, червей, троянских коней, программы-шпионы, вредоносные рекламные и другие программы для вмешательства в компоненты системы защиты и управления | Потеря доступности и конфиденциальности данных системы защиты и управления | Антивирусные программы, система сетевой защиты периметра, вайтлистинг и обнаружение вторжений.<br><br>Примечание 1: Остерегайтесь применения устойчивой смены / процедуры управления исправлениями, которая включает применение вайтлистинга.<br><br>Примечание 2: Вайтлистинг приложений имеет риск отказа при работе законных приложений системы защиты и управления, когда коды приложения были изменены (например, в результате исправления). |
| | Нечёткое тестирование: распространяет ошибочные случайные данные, которые мешают коммуникации системы защиты и управления | Потеря доступности и целостности данных системы защиты и контроля | Система сетевой защиты периметра и обнаружение заражения |
| Для имитации и модификации | Подмена: выдает себя за зарегистрированного пользователя или программу системы защиты и управления для получения доступа | Потеря конфиденциальности и целостности данных системы защиты и управления | Проверка подлинности системы защиты и управления на основе удостоверений, распространение ключей, IP-безопасность, и цифровые подписи |
| | Фальсификация: сознательное уничтожение или повреждение данных системы защиты и управления | Потеря целостности данных системы защиты и управления | Хэш-функции, при помощи проверки циклического избытка, сообщения с кодами аутентификации системы защиты и управления |

| Категории атак | Типы атак | Возможные последствия | Способы противодействия |
|---|---|---|---|
| | Клонирование: дублирование и переписывание действительных данных системы защиты и управления в эквивалентные данные | Потеря конфиденциальности данных системы защиты и управления | Физически не могут быть клонированы функции системы защиты и управления |
| | Повтор: запись и хранение ранее переданных данных системы защиты и управления для их повторения или задержки текущей сессии | Потеря конфиденциальности данных системы защиты и управления системы защиты и управления | Данные отметок времени в системе защиты и управления, времени синхронизации, псевдослучайных чисел, идентификаторы сессий, и серийных номеров |
| По сбору данных | Просмотр: быстрое чтение передаваемых сообщений системы защиты и управления для сбора данных | Потеря конфиденциальности данных системы защиты и управления | Шифрование и стеганография<br><br>Примечание: Стеганография-это искусство и наука писать скрытые сообщения таким образом, что никто, кроме отправителя и получателя, не подозревает о существовании сообщения, форма безопасности через неясность. |
| | Подслушивание: сбор сообщений системы защиты и управления | Потеря конфиденциальности данных системы защиты и управления | Шифрование, аутентификация личности в системе защиты и контроля и скрытое структурирование данных (CDA) |
| | Анализ передвижения: мониторинг обмена данными системы защиты и управления для определения схемы движения | Потеря конфиденциальности данных системы защиты и управления | Цифровая криминалистика системы защиты и управления и обнаружение неправомерного поведения |
| На конфиденциальные данные | Пользовательская: получение от пользователя системы защиты и управления информации о его местоположении, предпочтениях, поведении, и другой личной информация | Потеря конфиденциальности данных системы защиты и управления | Комплексное обеспечение защиты, анонимные передачи данных в системе защиты и управления, скрытое структурирование данных (CDA) и продвинутые электронные подписи<br><br>Пример: слепые, групповые или кольцевые подписи |
| | Корпоративная: установление функциональной ответственности,власти, и шпионажа в организации системы защиты и управления | Потеря конфиденциальности данных системы защиты и управления | Выборочное раскрытие информации, искажение данных системы защиты и управления |

### 3.2 Рекомендации для практических решений в системе защиты и управления

1. Будущие изменения в IEC 61850 должны включать конкретные требования по тестированию информационной безопасности для заводских приемочных испытаний, приемочные испытания и тестирование планового ремонта, как неотъемлемую часть нормального тестирования функционала.

2. Несмотря на тот факт, что антивирус беспомощен против атак нулевого дня, инженеры системы защиты и управления должны гарантировать актуальные исправления для защиты периметра системы защиты и управления, чтобы заблокировать известные угрозы.

3. В дополнение к антивирусной защите периметра, инженеры системы защиты и управления должны осуществлять политику вайтлистинга (белых списков), чтобы защитить доступ к системе защиты и управления и ее компонентам. Белый список – это утвержденный перечень или реестр с особой привилегией, услугами, мобильностью, доступом или признанием. Только лица, включенные в список, будут приняты, одобрены или признаны. Обратным белому списку является черный, в который определяются отвергнутые или не признанные.

4. Инженеры системы защиты и управления должны проверять все беспроводные удаленные доступы в системе защиты и управления. Не стоит недооценивать беспроводной доступ с использованием протокола обеспечения конфиденциальности (WEP), шифрование и интерфейс которого в системе защиты и управления объявлен “ненадежным”.[6]

5. Инженеры системы защиты и контроля должны получать ознакомительный курс информационной безопасности для улучшения их способности ощущать или обнаруживать индикаторы ошибок, для понимания подтекста этих индикаторов в рамках поведения приложений системы защиты и управления, предвидеть отклонения от предписанных мер защиты.

6. Инженеры системы защиты и управления и инженеры информационной сети должны рассмотреть и одобрить приемо-сдаточные испытания изготовителя (FAT) и приемочные испытания на месте эксплуатации (SAT), проверить планы и процедуры, чтобы гарантировать учет требований смягчения последствий в информационной безопасности.

7. Инженеры системы защиты и управления и инженеры информационной сети должны контролировать и проверять надлежащую безопасность конфигурации всех активов системы защиты и управления в окружающей среде подстанции, чтобы удостовериться в правильности параметров настройки.

8. Одна из областей улучшения - своевременное сообщение. Чтобы быть полезным для инженеров системы защиты и управления и для обеспечения согласованных сводок для управленческого надзора, отчеты должны содержать нормализованные данные. Важно коррелировать информацию из различных источников для определенных событий, данных и контекстов. Например, контроль сетевой безопасности системы защиты и управления, мониторинг активности пользователей и составления отчетов о соответствии.

9. Используя сканеры безопасности можно получить объективную оценку состояния информационной безопасности всей информационной системы. Выборочное сканирование обеспечивает оценку отдельных сайтов и приложений. Автоматизированное тестирование системы на предмет проникновения, система контроля и управления соответствует требованиям обеспечивающим непрерывный технический контроль безопасности на всех уровнях системы защиты и управления с информационной системой.

### 3.3 Десять основных замечаний

1. Объем и уровень информационной безопасности должны быть конкретными и соответствовать активам системы защиты и управления в условиях риска. Единый метод не всем подходит; риск-ориентированный выбор обеспечивает надлежащий контекст, который отвечает организационным структурам и политике.

2. Механизмы информационной безопасности должны быть широко распространенными, простыми, масштабируемыми и легкими в управлении инженерами системы защиты и управления в рамках своих обычных обязанностей.

[6] Смотрите раздел 4.2.3.8

3. Там, где это применимо, на основе оценки риска энергетической компании, электронная информация системы защиты и управления и приложения должны взаимодействовать с использованием открытых, защищенных протоколов, таких как те, что описаны в МЭК 62351.

4. Все приборы системы защиты и управления должны быть в состоянии поддерживать свою собственную политику информационной безопасности (или предоставленную охраной) на ненадежные сети.

5. Все инженеры системы защиты и управления, технический персонал и менеджеры, включая процессы, которыми они управляют, технология информационной безопасности, которую они используют, должно быть объявлено и иметь прозрачный уровень доверия для любого обмена данными.

6. Электронная информация системы защиты и управления должна быть соответствующих уровней (взаимной) аутентификации для доступа к системам и данным.
7. За пределами области управления системы защиты и управления, аутентификации, авторизации и учета необходимо внимательное отношение к надежности внешних интерфейсов.[4][7]

8. В соответствии с признаками, определенными в МЭК 62351, доступ к данным системы защиты и управления контролируется.

9. Конфиденциальность данных (и информационная безопасность любого актива системы защиты и управления, которая достаточно ценна) требует разделения обязанностей и привилегий, подкрепленных сильным управленческим доступом на основе ролей (RBAC) механизмов.

10. При хранении, перемещении или использовании, по умолчанию, включаются механизмы защиты данных системы защиты и управления.

# 4 Угрозы информационной безопасности систем защиты и управления

## 4.1 Введение в проблему угроз информационной безопасности

Сигналы, передаваемые по системе GOOSE (Generic Object Oriented Substantion Event – досл. «общее объектно-ориентированное событие на подстанции»), создает угрозу инициирования кибератаки, направленной против системы защиты и управления.

Необходимо рассмотреть различные виды кибератак. В разделе 4.3 представлен обзор важнейших уязвимых мест и атак (так называемая карта угроз). Раздел 4.4 посвящен рассмотрению вопроса «Предоставляют ли сигналы, передаваемые системой GOOSE, возможности для совершения кибератаки против системы защиты и управления?» Раздел 4.5 концентрируется на уязвимостях неподключенных и защищенных систем. Раздел 4.6 посвящен урокам, которые можно извлечь из истории с распространением компьютерного вируса Stuxnet. В разделе 4.7 описываются потенциальные риски для систем защиты и управления и противоаварийной автоматики (ПА). В приложении P приводится обзор доклада Совета по развитию науки и техники при Президенте США (PCAST) «Текущие возможности для усиления национальной безопасности в киберпространстве» *Immediate Opportunities for Strengthening the Nation's Cybersecurity [5]*.

## 4.2 Реальные угрозы системам защиты и управления

### 4.2.1 Введение в проблему реальных угроз системам защиты и управления

[7] Объектом доверия в сети организации рассматривается несколько документов, включая цитируемую ссылку.

Настоящий пункт состоит из двух частей. Первая часть описывает различные типы уязвимостей, которые возникают в процессе развития систем защиты и управления (как аппаратного, так и программного обеспечения), а вторая часть описывает уязвимости, которые возникают в процессе внедрения и эксплуатации систем защиты и управления. Тема инсайдерских угроз отдельно не освещается, поскольку подразумевается, что данный тип угроз имеет отношение к каждой из уязвимостей, описанных в пункте 4.2. Инсайдер определяется как взломщик, изначально обладающий определенной степенью доверия, и за счет чего способный произвести разведку. Помимо всего прочего, приведенный анализ допускает наличие формальных и неформальных проявлений доверия к персоналу, которые могут иметь как материальную, так и нематериальную форму.

### 4.2.2 Уязвимости, возникавшие в ходе развития

#### 4.2.2.1 Введение в проблему уязвимостей, связанных с развитием

Уязвимости, заложенные в аппаратное и программное обеспечение изготовителями систем защиты и управления обычно являются наиболее сложными для выявления и устранения инженерами систем защиты и управления в электроэнергетических компаниях. Наиболее распространенный недостаток систем защиты от кибератак[8] представляет собой уязвимость, предоставляющую возможность ввода вредоносного кода в программное обеспечение системы защиты и управления [6].

Важнейшая причина, по которой данный вид атаки стоит принять во внимание, является тот факт, что вышеуказанная уязвимость позволяет отдельным лицам обойти ограничения системы управления доступом, накладываемые разработчиком или инженером системы защиты и управления в электроэнергетических компаниях (EPU) и, например, удаленно получить полный контроль над защитным реле или расширить полномочия пользователя до полномочий администратора защитного реле (обычно, последнее предполагает возможность вносить изменения в полномочия других пользователей).

Атаки, связанные с вводом кодов, могут быть реализованы в форме ввода бинарного или исходного кода [7].

#### 4.2.2.2 Атаки переполнения буфера

Атака в форме ввода бинарного кода предполагает использование вредоносного кода в целях изменения поведения программы. Подобные атаки часто реализуются посредством переполнения буфера. [8] (сравните с приложением H)

Атаки переполнения буфера были открыты в 1980-х гг.. В теории считается, что подобного рода атаки относительно несложно нивелировать. Однако, в связи с существованием практических ограничений, в действительности данная проблема, теоретически как будто бы легко решаемая, оказывается довольно непростой. Уязвимости, создающие угрозы переполнения буфера, почти ежедневно обнаруживаются во всех видах стандартного программного обеспечения. И программное обеспечение систем защиты и управления не является исключением.

Среди причин, обусловливающих вышеописанную проблему, можно выделить недостаточную осведомленность разработчиков программного обеспечения систем защиты и управления в области мер безопасности, а также высокую степень сложности современного стандартного программного обеспечения. [9]

Последствием успешных атак переполнения буфера, как правило, являются отказ в обслуживании или приобретение определенных привилегий.

#### 4.2.2.3 Внедрение кодов

Различные способы внедрения кодов включают следующие виды уязвимостей, или слабостей:

[8] Вставка вредоносного кода пользуется непроверенными предположениями, которые делает программное обеспечения системы защиты и управления при вводе данного кода - смотрите цитируемую ссылку.

- межсайтовые запросы;
- внедрение SQL-кода;
- внедрение облегченного протокола доступа к сетевому каталогу (LDAP);
- внедрение команд в SMTP/IMAP сессию;
- внедрение нулевого байта в строку;
- внедрение команд в операционную систему;
- внедрение специальных символов в файловые пути (обход директорий);
- исполнение внешнего файла;
- внедрение в серверную часть;
- внедрение расширяемого языка разметки (XML);
- внешние источники;
- внедрение в различные участки XML-документов различных типов;
- внедрение в различные участки документов на языке запроса XQuery.

Данная техническая брошюра обращается только к таким видам угроз, как межсайтовые запросы и внедрение SQL-кода.

Атаки, связанные с внедрением исходного кода, предполагают взаимодействие с системными приложениями, написанными на не требующих компиляции языках программирования, таких как JavaScript, Гипертекст (PHP) и языке структурированных запросов (SQL). В связи с указанным обстоятельством, атаки рассматриваемого вида в первую очередь касаются веб-приложений. Наиболее распространенные уязвимости данной категории включают в себя межсайтовые запросы (XSS) (смотрите приложение F) и внедрение SQL-кода. Межсайтовые запросы предполагают внедрение вредоносного JavaScript-кода в существующие веб-приложениям, что впоследствии предоставляет каждому посетителю (или определенным посетителям, указанных взломщиком) возможность совершать определенные действия.[9]

Внедрение вредоносного SQL-кода позволяет взломщику получить доступ к серверной базе данных в обход средств, предусмотренных для этого разработчиком системы защиты и управления. К примеру, уязвимость, связанная с угрозой внедрения SQL-кода может дать взломщику возможность извлечь содержимое базы данных системы защиты и управления или получить полный контроль над системой защиты и управления.

### 4.2.3 Уязвимости, возникающие на этапе внедрения и технической эксплуатации

#### 4.2.3.1 Введение в проблему уязвимостей, возникающих на этапе внедрения и технической эксплуатации

На этапе внедрения систем защиты и управления и управления такими системами могут возникать различные виды уязвимостей, которые заслуживают внимания. Наиболее распространенный тип уязвимостей подобного рода связан с программными сервисами, которые либо не используются, либо недостаточно освоены инженерами, несущими ответственность за безопасность систем защиты и управления [10].

Неиспользование определенных функциональных возможностей программного обеспечения, либо недостаточная осведомленность инженеров систем защиты и управления относительно таковых представляют собой серьезную проблему, поскольку дают взломщику возможность нарушить нормальное функционирование системы защиты и управления. Рассматриваемые в настоящем пункте виды программных сервисов являются наиболее уязвимыми, поскольку никто обычно не занимается их защитой. Примером сервиса, который часто встраивается в систему защиты и управления, но редко используется, может служить сервис совместного доступа к файлам в системе Windows, который по умолчанию предусмотрен в современной ОС Windows. В качестве примера сервиса, незнакомого оператору систем защиты и управления, можно рассматривать протокол передачи данных (FTP), который способен предоставлять пользователю удаленный доступ к файлам системы защиты и управления без согласования с инженером системы защиты и

[9] В литературе, которая находится в открытом доступе, крупные компании рекламируют веб-сайт для удаленного управления автоматикой подстанции.

управления.

#### 4.2.3.2 Проблема доверия при предоставлении удаленного доступа

Инженеры систем защиты и управления, технологи и управляющие должны выработать прозрачную систему уровней доверия для любого обмена данными, имеющего места при функционировании системы, включая контроль технологических процессов и технологии защиты от кибератак. В связи с этим нельзя полагаться на средства комплектования и эксплуатации оборудования систем защиты и управления, к которым можно получить доступ из внешней по отношению к подстанции[10] среды, такие, как интеллектуальные электронные устройства (ИЭУ), блоки дистанционного управления (RTU) и программируемые логические контроллеры (PLC) [10].

#### 4.2.3.3 Ошибки при настройке брандмауэра

Принимая во внимание тот факт, что брандмауэр на подстанции устанавливается на маршрутизаторе, или на роутере локальной сети (LAN), его правильная настройка является сложной задачей для оператора системы защиты и управления вследствие сложности правил брандмауэра. Такая настройка представляет собой существенную проблему не только на стадии установки системы и ввода ее в эксплуатацию при проведении приемочных испытаний (SAT) на соответствие техническим условиям, но также и на стадии эксплуатации на протяжении всего жизненного цикла системы автоматизации подстанции.[11]

Поскольку брандмауэр размещается на внешнем интерфейсе подстанции (например, в центре управления или в удаленном инженерно-техническом центре), настройка брандмауэра не входит в обязанности оператора системы защиты и управления. Однако, последний должен быть уверен, что брандмауэр настроен правильно, поскольку на его надежность возлагаются большие надежды. В целях достижения такой уверенности, правильность настройки должна подтверждаться результатами приемочных испытаний (SAT) и эксплуатационных испытаний .

Независимо от месторасположения брандмауэра, частые ошибки в его настройках предоставляют взломщикам возможности получить доступ к уязвимым компонентам системы защиты и управления и их содержимому. [11]

#### 4.2.3.4 Подбор пароля в режиме онлайн

Одна из наиболее распространенных ошибок в настройках позволяет осуществить подбор паролей в режиме онлайн. В рамках программного обеспечения систем защиты и управления, использующего пароли, должна быть предусмотрена функция, ограничивающая допустимое количество попыток ввода пароля (обычно – максимально три попытки). Если такая функция отсутствует, взломщики могут получить доступ, пройдя механизм проверки подлинности путем подбора. Ненадежность пароля влечет возникновение существенной уязвимости, поскольку в таком случае злоумышленник легко может подобрать пароль, используя словарь общеупотребительной лексики.

Надежный пароль, как правило, характеризуется непредсказуемостью [12] и может быть составлен путем использования эвристического подхода [13]. Пароль по умолчанию легко подобрать, если они ненадежны (например, «администратор») или записаны в доступном для взломщика месте (например, указаны в документах поставщиков электроэнергии, размещаемых в общем доступе). Операторам систем защиты и управления следует использовать приведенные рекомендации, чтобы удостовериться в надежности паролей доступа к системам защиты и управления и сетям подстанций и в их соответствии правилам обеспечения безопасности в электроэнергетических компаниях (EPU).

Однако стоит предупредить, что действия в аварийной ситуации могут потребовать отключения функции, ограничивающей количество попыток ввода пароля. В таком случае, оператор системы защиты и управления должен удостовериться, что данная функция отключается в соответствии с рабочими практиками эксплуатации системы. Кроме того, доступ к активации и деактивации

[10] http://www.wired.com/threatlevel/2012/01/10000-control-systems-online

[11] http://www.us-cert.gov/control_systems/csvuls.htm#data.

функции должен быть защищен сильным шифром.

#### 4.2.3.5 Подбор пароля в режиме оффлайн

Иногда взломщики способны изымать целые базы данных с пользовательскими параметрами доступа, например, с сервера активных каталогов. Если информация закодирована ненадежно, или совсем не закодирована, злоумышленник может просто извлечь ее из базы данных. Если информация характеризуется низким уровнем энтропии, (то есть предсказуемостью), она может быть извлечена даже из надежно закодированной базы данных. По этой причине инженерно-технические руководители систем защиты и управления должны обеспечивать соблюдение необходимых мер обеспечения безопасности от кибератак, а также организационных распорядительных документов.

#### 4.2.3.6 Несоответствие требованиям контроля доступа

Недостаточная спецификация правил контроля доступа может привести к тому, что пользователи системы защиты и управления получают чрезмерные или недостаточные полномочия. Примером такой ситуации может послужить предоставление доступа с правами администратора лицу или группе лиц, которым следовало бы предоставлять доступ типа «только для просмотра». Доступ с правом записи информации и изменения настроек представляет собой серьезное нарушение политики безопасности в области контроля доступа.[12] Чрезмерная концентрация системы контроля доступа на ограничении также может привести к проблемам из-за того, что сервисы управления данными не закрываются надлежащим образом или из-за того, что сотрудники делятся между собой параметрами доступа, представляющими значимость для безопасности системы.

Операторы систем защиты и управления должны регулярно перепроверять, какие полномочия с точки зрения контроля над доступом имеет каждый сотрудник и следить за тем, чтобы эти полномочия должным образом согласовывались с должностью и кругом обязанностей.

#### 4.2.3.7 Психологические атаки

Важно помнить, что кибератака необязательно должна быть связана с использованием вредоносного кода. Нередки случаи компьютерного мошенничества, которое увенчивается успехом благодаря тому, что особо важная информация, содержащаяся в системе защиты и управления невольно подвергается разглашению вследствие отсутствия обучения в области безопасности [14]. Часто применяются такие способы психологической атаки, как телефонные звонки с целью заставить оператора системы защиты и управления загрузить вредоносную программу или электронную почту, содержащую вредоносные коды, или направить оператора на мошеннический веб-сайт [15,
16]. Последний из упомянутых способов называют фишингом, если он не направлен против конкретного лица или электроэнергетической компании. В противном случае описанный способ называется целевым, или выборочным фишингом[17].

Операторы систем защиты и управления должны соблюдать меры предосторожности при переговорах с поставщиками технических решений для систем. На вебинарах, конференциях и семинарах специалистов часто заманивают детальными описаниями новых технологий, позволяющих расширить функциональные возможности систем защиты и управления электроэнергетических компаний. Регулярное обновление знаний в области безопасности позволит операторам систем защиты и управления лучше распознавать угрозы психологических атак.

#### 4.2.3.8 Сетевой трафик: анализ и управление

Злоумышленник, способный перехватывать и записывать данные в процессе передачи, имеет потенциальную способность совершить целый ряд различных атак. Например, он может повторно отправить ранее переданные сообщения и тем самым создать у системного оператора ложное представление о состоянии энергосистемы [18, 19]. Также злоумышленник может отправить исправленные сообщения. Такие действия называются «атакой с перехватом» [20].

[12] http://industryconsulting.org/pdfFiles/NIST%20Draft-SP800-82.pdf

Нетрудно также осуществить перехват паролей, передаваемых в незашифрованном виде. Такой перехват обеспечит возможность получить доступ к системе защиты и управления. Очевидным результатом описанных действий будет нарушение целостности системы защиты и управления. Однако, применение выбранной случайным образом системы кодирования не является достаточной мерой для предотвращения злонамеренного перехвата и записи потока сообщений.

Рекомендуется уделять повышенное внимание выбору внедряемой беспроводной связи, хотя, разумеется, это относится также и к проводным средствам связи. Примером данной угрозы может служить использование в электроэнергетических компаниях (EPU) беспроводных сетей стандарта IEEE 802.11, использующих протокол обеспечения конфиденциальности (WEP), поскольку система шифрования указанного протокола может быть легко взломана.[13]

Инженеры систем защиты и управления должны быть ознакомлены со всеми беспроводными технологиями удаленного доступа к системе. Следует избегать использования беспроводного доступа к системе защиты и управления с использованием шифрования протоколом обеспечения конфиденциальности (WEP), поскольку данный протокол в настоящее время объявлен «незащищенным».

### 4.3 Карта угроз и отбор наиболее вероятных угроз

В таблице 2 все виды уязвимостей, описанные в подпунктах 4.2.2 и 4.2.3, соотносятся с различными видами устройств системы защиты и управления.

Если система связывает активы (отмеченные "x") с определенной уязвимостью, то этот актив может потенциально содержать такой недостаток. Например, злоумышленник может использовать недостаток информированности по вопросам безопасности персонала с помощью психологической атаки, чтобы получить имя пользователя и пароль техника подстанции. Как правило, число потенциальных уязвимостей возрастает с функционалом данного актива. Персональный компьютер (ПК) со стандартной операционной системой включает в себя большое количество функций; например, Microsoft Windows 7 имеет больший вектор атаки, чем маршрутизатор с несколькими рудиментарными функциями.

Таблице 2 не детализирует вероятность любой из этих уязвимостей. Уязвимости переполнения буфера могут быть менее очевидным на ИЭУ, чем на ПК, так как программное обеспечение ИЭУ, в основном, менее сложное, чем программное обеспечение ПК. Как правило, чем меньше количество строк кода, тем ниже вероятность ошибки со стороны разработчиков программного обеспечения.

Другим важным понятием, не указанным в таблице 2, является тяжесть различных следствий в результате использования уязвимости. Например, подбор пароля в режиме оффлайн может быть несерьезной проблемой для многих систем защиты и управления, так как это в этом случае взломщику необходимо иметь некоторые привилегии в системе. В свою очередь, недостаточный доступ и использование элементов управления могли бы создать большие проблемы, так как это позволило бы лицам, которые не разбираются в информационных технологиях совершать успешные вторжения.

Такой же тип использования может привести к различным последствиям для других активов системы защиты и управления. Например, человеко-машинный интерфейс (HMI) системы защиты и управления на подстанции не позволяет просмотр веб-страниц (фильтры брандмауэра), тем самым улучшает защиту. В частности, переполнение буфера в веб-браузере человеко-машинного интерфейса (HMI) менее проблематично, чем в случае с компьютером, который подключен к

[13] Хотя его название подразумевает, что он также безопасен, как проводное соединение, протокол обеспечения конфиденциальности (WEP) имеет множество недостатков и является устаревшим по отношению к новым стандартам, таким как WPA2. В 2003 году Wi-Fi Alliance объявила о том, что Wi-Fi Protected Access (WPA) вытесняет стандарт WEP. В 2004 году при ратификации полной версии стандарта 802.11i (т.е. WPA2), IEEE заявил, что оба стандарта WEP-40 и WEP-104 ", объявлены устаревшими, поскольку они не в состоянии достичь своих целей безопасности".

подстанции через локальную сеть.

Более того, компьютерное вторжение в той же категории и того же актива может также привести к очень разным последствиям. Например, неизвестная служба удаленного подключения (например, протокол удаленного рабочего стола (RDP), система управления удаленным компьютером (VNC), безопасная оболочка (SSH) или Telnet) с соответствующим ей слабым паролем обычно более надёжна, чем неизвестный сервер с протоколом передачи данных (FTP).

В заключении, руководители системы защиты и управления не должны рассматривать эти уязвимости активов системы защиты и управления независимо, так как успешные кибератаки, как правило, включают в себя использование цепочки уязвимостей, присутствующих в различных активах. Например, многие атаки с помощью психологической атаки включают электронные письма, содержащие ссылки на сайты с наборами для вторжения. В сущности, злоумышленник должен выполнить две задачи:

1) провести психологическую атаку на персонал, чтобы открыть ссылку в письме, и
2) использовать уязвимость в веб-браузере (наиболее вероятно переполнение буфера) для подключения.

Следовательно, возникает необходимость моделировать и анализировать совокупность систем для оценки относительной безопасности при опасных действиях злоумышленника.

## Таблица 2 Карта угроз системы защиты и управления

| Уязвимость | Ресурс системы защиты и управления | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | ИЭУ/RTU/PLC | Человеко-машинный интерфейс | Входной канал | Роутер или переключатель | Цифровой регистратор аварий | Пункт укладки кабеля локальной сети | Инженер системы защиты и управления | Единица измерения | Брандмауэр | Собственные устройства (смотрите приложение E) |
| Переполнение буфера | X | X | X | X | X | | | | X | X |
| Межсайтовые запросы | X | | | | | | | | | |
| Ложные программные службы | | X | | | | | | | | X |
| Ложная точка доступа | X | X | | | | X | | | | X |
| Ошибки при настройке брандмауэра | | | | | | | | | X | |
| Подбор пароля онлайн | X | X | X | X | X | | | X | X | X |
| Подбор пароля оффлайн | | | | | | | | | | X |
| Несоответствие требованиям контроля доступа | X | X | X | X | X | | | X | X | X |
| Психологическая атака | | | | | | | X | | | |
| Анализ и управление сетевым трафиком | | | | | | X | | | | |
| Заменяемый драйвер | X | X | X | | | | | | | X |
| Атаки лавинной адресации сообщений | X | X | X | X | X | X | | X | X | X |

## 4.4 Предоставляют ли сигналы, передаваемые знаменитой системой GOOSE, возможности для совершения кибератаки против системы защиты и управления

### 4.4.1 Применение системы GOOSE для защиты

МЭК 61850 дал начало концепции обмена сообщениями GOOSE (общие объектно-ориентированные события подстанции). МЭК 61850-8-1 является его основной спецификацией. На сегодняшний день пакет кадров Ethernet (уровень 2) формирует GOOSE сообщения. GOOSE представляет собой сообщение об изменении состояния многоадресной рассылки, которое генерируется и публикуется из ИЭУ ко всем пользователям по локальной сети подстанции - шине электростанции. Кроме того, при обмене информацией между подстанциями для реализации важных функций защиты и управления энергетической системы используются системы связи на основе GOOSE. Их применение зависит от технологического процесса в системе МЭК 61850. Технический отчет МЭК / TR 61850-90-1 описывает этот сценарий. Возможные функции защитных GOOSE приложений включают в себя отключение выключателя, запуск отказа выключателя, автоматическое поворотное включение между реле и выключателем, размыкание между двумя реле, и взаимоблокировку блоков управления присоединениями и реле.

Примерами критериев производительности GOOSE сообщений, определенных в МЭК 61850-5, являются: 3 мс для изменения состояния информации и 20 мс для блока информации. При данном требовании для отправки сообщения в интервале 3 мс, одной из основных проблем является задержка, которая появляется в результате добавления шифрования для защиты конфиденциальности полезных данных GOOSE. Обязательные механизмы безопасности, указанные в предстоящем новом выпуске МЭК 62351-6 [21], предназначены для защиты целостности сообщений GOOSE, то есть, для подтверждения, что сообщение приходит из законного источника и не изменено. В МЭК 62351-6, шифрование сообщений для достижения конфиденциальности не является обязательным. Эффективность использования зависит от лежащих в основе требований к производительности и аппаратному обеспечению, а также шифровальной способности. Помимо требований МЭК 62351, мощная сеть безопасности обеспечивает многослойную защиту критически важного GOOSE трафика. Виртуальная локальная компьютерная сеть (VLANS) для разделения трафика в пределах подстанции, технологии виртуальной частной сети(VPN) для разделения распределенной сети (WAN) и шифрования, а также защита портов на основе IEEE 802.1x являются сильными средствами достижения серьезного уровня безопасности. Все службы и управления, включая брандмауэр и IDS / IPS (систему обнаружения вторжений / систему предотвращения вторжений) систем, должны быть частью архитектуры защиты для данной системы.

Если серьезное нарушение вызвано виртуальным мероприятием, необходимы комплексные меры по снижению риска для сведения последствий к минимуму.

### 4.4.2 Маршрутизированный GOOSE и выборочные значения для передачи информации устройств синхронизированных векторных измерений

Профиль сообщения «маршрутизированного GOOSE» определен в МЭК / TR 61850-90-5[14] [22]. Данный профиль сообщения вводит сеансовый уровень для формирования пакета данных и передачи сообщений приложения, в соответствии с МЭК 61850-9-2 [23] для выборочных значений и МЭК 61850-8-1 [24] при использовании протокола дейтаграмм пользователя (UDP) / сервисов групповой адресации IP. Новое преобразования для технологий групповой адресации IP, которое может быть интегрировано в серии стандартов МЭК 61850, распространяется на возможности IP-сетей, а также на лежащие в их основе сценарии использования эффективного соединения одного абонента с несколькими.

В дополнение к определениям протокола обмена данными, МЭК / TR 61850-90-5 содержит защитную модель, которая определяет как функции шифрования, так и управление ключами. Он описывает обязательные требования к аутентификации, целостности информации и дополнительные требования к ее конфиденциальности.

[14] IEC/TR 61850-90-5 описывает протокол передачи информации устройств синхронизированных векторных измерений.

Часть 90-5 нормирует использование защищенного хеш-кода аутентификации сообщений (HMAC) по всей информации протокольного блока данных сеансового уровня (SPDU), с использованием ключей шифрования. Более того, часть 90-5 протокола сеанса связи поддерживает возможность шифрования полезной информации протокольного блока данных сеансового уровня (SPDU).

Кроме того, защитная модель включает в себя определения безопасности, как описывается в МЭК 62351-6:2007, для обеспечения комплексной безопасности. С учетом запланированных обновлений, данный стандарт определяет безопасность МЭК 61850 GOOSE и данных выборочных значений, которые рассматриваются в разделе 4.4.2. Для удовлетворения стандартных требований, защитная модель обеспечивает гибкий подход в контексте таких определений, как периметры физической защиты (PSP) и периметры электронной защиты (ESP).

Помимо спецификации безопасности с точки зрения целостности, аутентификации и конфиденциальности, часть 90-5 описывает управление групповым ключом, которое основано на группе доменов интерпретации (GDOI) в соответствии с запросом на комментарий (RFC) 3547 [25]. Данная концепция вводит "совершенную прямую" безопасность, чередование ключа и использование центра распределения ключей (KDC), в централизованном или децентрализованном сценарии развертывания. Концепция центра распределения ключей (KDC) поддерживает управление ключами и обмен с помощью механизмов, инициирующих запросы от пользователя и от сервера.

План состоит в том, чтобы интегрировать спецификацию безопасности части 90-5 в соответствующие части серии МЭК 62351, как вклад в усилия по обеспечению комплексной безопасности 15ой рабочей группы МЭК ТС 57. В качестве примера, спецификации управления ключами основанные как на группе доменов интерпретации (GDOI), так и на концепции центра распределения ключей (KDC) будут включены в новый стандарт МЭК 62351-9 (Key Management) [26]. По существу, "маршрутизируемый" профиль не только будет обеспечивать новые возможности для связи и топологической сети (например, групповая адресация IP), но также будет предлагать расширенные возможности безопасности для защиты IP-трафика и будет ограничивать домены аварийных ситуаций в сценариях взаимодействия между подстанциями.

## 4.5 Уязвимости в неподключенных и защищенных системах

### 4.5.1 Введение

Общеизвестно, что выход в интернет общего пользования сопряжен с множеством угроз. В связи с этим, необходимость проведения ограничительных и превентивных мероприятий по обеспечению безопасности систем защиты и управления, имеющих выход в интернет общего пользования на интуитивном уровне очевидна для каждого, кто имеет какое-либо отношение к информационной безопасности систем защиты и управления. Однако предполагать, что система защиты и управления, изолированная от доступа в интернет общего пользования, полностью защищена, ошибочно. Даже для таких систем, которые объединены только с теми системами, которые признаются защищенными, или ни с чем не объединены, могут существовать серьезные уязвимости и риски. Уверенность в надежности так называемого «воздушного зазора», или физической изоляции, между системой защиты и управления и сетью интернет не учитывает существенных угроз со стороны непрямо присоединенных систем, неподключенных систем, а также систем, признанных достоверными и защищенными, однако обладающих серьезными скрытыми конструктивными недостатками. В данном разделе описываются потенциальные уязвимости неподключенных и защищенных систем для помощи разработчикам систем защиты и управления разобраться в данной категории угроз, которые зачастую игнорируются вследствие низкой вероятности их возникновения. Принятие во внимание рассматриваемых угроз и поиск путей их устранения позволит разработчикам добиться большей гибкости систем защиты и управления, которая даст возможность им успешно функционировать даже в аномальных условиях, не предусмотренных при разработке системы.

### 4.5.2 Миф о физической изоляции системы защиты и управления

Хотя принято считать, что в энергетических компаниях изменения происходят медленно,

современные электроэнергетические компании не слишком сильно отличаются от прочих предприятий в вопросах широкого применения взаимосвязанных вычислительных систем. Объединение внутренних систем посредством сетевых технологий позволяет получить существенные коммерческие выгоды. Благодаря связности сетей можно добиться значительного повышения производительности, чем современные предприятия пользуются для поддержания конкурентоспособности.

Во избежание дополнительных расходов на обеспечение защиты систем защиты и управления, некоторые эксперты предлагают отсоединять ее от других систем. Таким образом, если система защиты и управления не подсоединена к другим системам, это обусловлено стремлением избежать издержек на ее защиту. Это может привести к тому, что в системе при ее установке не предусмотрено никаких мер по контролю безопасности.

Однако тот факт, что физическая изоляция сетей будет сохраняться на протяжении всего жизненного цикла систем защиты и управления, представляется маловероятным. Обусловленные бизнесом факторы стимулируют повсеместное соединение сетей на предприятиях. Это касается также и систем защиты и управления. В связи с продолжающейся тенденцией к удешевлению соединения сетей можно предположить, что стимулы к его внедрению будут увеличиваться. В итоге это приведет к тому, что со временем системы защиты и управления придется соединить с другими системами и компьютерами предприятия.

Как только происходит такое соединение, появляется реальная возможность связей между системой защиты и управления и другими системами или компьютерами, которые могут носить нежелательный характер. Даже если сама система защиты и управления или другие системы, с которыми она связана, не имеют прямого подключения к Интернету общего пользования, вероятность каких-либо нежелательных контактов существенно повышается.

В связи с изложенным, полагаться на физическую изоляцию систем защиты и управления как на меру их защиты небезопасно. Необходимые меры по обеспечению безопасности защиты и управления должны предприниматься уже на этапе разработки, в противном случае, по истечении определенного срока эксплуатации указанные меры становятся более трудоемкими и дорогостоящими. Невозможность построения абсолютно безопасных систем защиты и управления приводит к возникновению серьезных скрытых уязвимостей. Если система защиты и управления имеет первостепенное значение для защиты какой-либо важной единицы оборудования, угроза безопасности которой может оказать негативное воздействие на готовность или целостность всей энергосистемы, необходимо провести мероприятия, направленные на обеспечение безопасности таких систем защиты и управления уже на этапе разработки и внедрения. Это не значит, что все системы защиты и управления должны предполагать защиту от прямого подключения к Интернету общего пользования. При этом нельзя игнорировать возможность нежелательного контакта с внешними системами. При разработке системы защиты и управления необходимо принять во внимание возможность непредвиденных контактов, которые могут носить недостоверный характер. Все запросы на осуществление управляющих действий необходимо предварительно оценивать с точки зрения последствий требуемого действия, даже если они исходят от неподключенной или достоверной системы.

### 4.5.3 Неподключенные системы

#### 4.5.3.1 Введение

Полностью неподключенные компьютерные системы уязвимы для угроз безопасности. Неподключенными системами являются такие системы, которые не имеют подключения к внешней системе. Они могут состоять из ИЭУ без какой-либо связи, компьютера, без подключения к сети, или из совокупности компьютера с человеко-машинным интерфейсом (HMI), независимо подключенного к ИЭУ по выделенному каналу. В том время как полностью неподключенная система может и не подвергаться вредоносным или нежелательным сообщениям с ресурсов интернета, эти системы могут быть уязвимы для разнообразных угроз, некоторые из которых будут описаны ниже. В то время как уязвимости не могут иметь отношение к каждой системе защиты и управления, защита против них требует надлежащей практики безопасности как внутри подстанции, так и от тех, кто мог бы подключиться к системе. Только при понимании этих

потенциальных угроз, электроэнергетические компании могут разработать эффективную практику защиты.

#### 4.5.3.2 Уязвимости порта USB

Несмотря на то, что не имеющее USB порт ИЭУ может казаться защищенным от направленных на USB порты атак, ИЭУ не обязательно должно иметь USB порт, чтобы подвергнуться атакам такого типа. В отличие от ИЭУ, HMI обычно создаются на более универсальных вычислительных платформах. Эти платформы обычно поддерживают USB порты. Во многих случаях USB порт является важной частью функционирования HMI, которая позволяет изменять настройки и другие конфигурационные данные, необходимые для работы системы защиты и управления на подстанции. По причине уязвимости USB порта, подвергнутый угрозе HMI ставит под угрозу и ИУЭ и всю систему защиты и управления (см. раздел 4.6). Аналогично, если ИУЭ имеет USB порт, то уязвимые места могут быть различными, и это, тем не менее, влияет на исправность всей системы защиты и управления. Уязвимость любого отдельного компонента и не только его, но и других компонентов, к которым он подключен, ставит под угрозу исправность всей системы. Влияние на разработку систем защиты и управления - это возможность того, что не связанные между собой системы могут быть подвергнуты воздействию непредвиденного программного обеспечения, которое может привести к несоответствующим и/или вредоносным управляющим воздействиям. Подвергнутый угрозе HMI через USB порт может поставить под угрозу ИЭУ и всю систему защиты и управления (см. раздел 4.6).

#### 4.5.3.3 Непредвиденные подключения к сети

Связь становится широко распространенной и неограниченной. Даже в пределах одной подстанции без внешнего подключения к общей сети (т.е. нет маршрутизатора подстанции, как показано на схеме 1), существует возможность непредвиденного подключения к сети в связи с широким распространением беспроводных сетей. Кроме самых удаленных подстанций, почти каждая городская подстанция на планете, способна принимать сигналы сотовой связи. Подстанции, находящиеся в непосредственной близости от жилых домов и административных зданий, могут получать их Wi-Fi сигналы. Инженер, который принес ноутбук на подстанцию и вошел в сеть подстанции для осуществления технического обслуживания, может непреднамеренно подключиться к этим системам и тем самым сделать систему защиты и управления незащищенной от нежелательного подключения к внешней системе.

Возможность появления непредвиденных сетевых подключений должна представлять интерес для разработчиков системы защиты и управления, потому что большинство протоколов системы защиты и управления – это не аутентифицированные протоколы, которые, по всей вероятности, могут определить отправителя управляющих команд. Такие протоколы, как МЭК 60870-5-101 / 104, DNP 3 или МЭК 61850 имеют дополнительные возможности поддержки строгой аутентификации. Однако эти опционные возможности редко встречаются внутри систем защиты и управления. В результате, когда ИЭУ получает сообщение из сети подстанции для выполнения управляющего действия, ИЭУ не имеет возможность гарантировать, что лицо, пославшее сообщение, является тем, от кого ИЭУ это сообщение ожидало. Вместо этого большинство ИЭУ безоговорочно доверяют полученным сообщениям без проведения надлежащей аутентификации, если она вообще проводится. Задачи, связанные с внедрением полностью аутентифицированной связи в систему защиты и управления, являются значительными и могут быть практически нереализуемы в связи со сложностью выполнения и стоимостью (смотри раздел О.5). В то же время, просто предполагая, что все подключения являются действительными, они отходят от системы защиты и управления излишне уязвимыми для всех несоответствующих сетей, даже если сети не являются вредоносными. Разработчик систем защиты и управления должен учитывать последствия непредвиденного обмена сообщениями, особенно при использовании не аутентифицированных протоколов. Не прошедшие данную проверку управляющие воздействия требуют проверки перед их выполнением.

### 4.5.4 Уязвимости доверенных систем

Применительно к данному анализу, доверенный компонент является одним из компонентов, содержащихся в системе защиты и управления, который всегда создает сообщения, отражающие реальное состояние системы и действительные запросы управления. Традиционно, любой компонент в системе защиты и управления становится доверенным после финального тестирования подстанции перед вводом подстанции в активную эксплуатацию. Как только подстанция входит в эксплуатацию, конфигурация и программирование системы защиты и управления предполагает, что все взаимодействующие компоненты становятся доверенными. Конечно, нельзя сказать, что игнорируются проверки правильности уровней сигнала, качества сигнала, диапазон допустимых значений, блокирование, маркировка, нарушение связей и т.д. Качественная разработка системы защиты и управления всегда включала в себя фундаментальные механизмы проверки и безопасности данных в целях обеспечения безопасных и целесообразных решений по управлению. Например, рассмотрим случай, когда полученная с другого участка оценка состояния системы имеет хорошее качество и надлежащую временную отметку, а так же показывает, что автоматический выключатель на другом участке открыт. Большинство ИЭУ будут предполагать, что этот автоматический выключатель действительно был открыт и, что полученная ими оценка состояния отражает реальное состояние электроэнергетической системы, и после предпримут соответствующие меры управления, на которые были запрограммированы в этого случае.

А что, если полученная информация не отражает истинного состояния электроэнергетической системы? Как уже говорилось выше, неправильные или даже вредоносные сообщения могут встречаться. Приняла бы система защиты и управления другое решение по управлению, если бы системы были больше ненадежными, чем доверенными? Если обмен неправильными или вредоносными сообщениями – возможная реальность, повлияет ли это на функции защиты системы защиты и управления. Если используемая система имела большое значение для готовности и исправности электроэнергетической системы, то вероятно, что разработчик системы защиты и управления рассмотрит возможность уменьшения негативных последствий. Возможности уменьшения последствий могут включать в себя дополнительный сигнал в алгоритмах обработки команд или независимые дополнительные функции защиты.

Является ли применение доверенных систем ошибкой проектирования? Этот вопрос, поднятый в 2007 году, посредством противоречивой демонстрации «Авроры», проведенной Национальной Лабораторией Айдахо, был широко освещен на CNN[15]. В ходе проведения демонстрации на систему управления генератором подавались управляющие вредоносные команды, которые, в конце концов, сильно повредили генератор. В данном случае система управления генератора полагала, что все полученные команды были корректными, и выполняла их без учета того, приведут ли они, в конечном счете, к потере синхронизма и повреждению генератора.
Пренебрежение возможностью уменьшения последствий атак на систему информационной безопасности позволило отправить из интернета вредоносные управляющие сигналы на генератор. Меры по смягчению уязвимости включают в себя независимую систему защиты, которая отключает генератор при появлении попыток подключения в асинхронном режиме[16]. Лица, выступающие за результаты демонстрации, заявили, что пренебрежение обеспечением независимой защиты в генераторе является серьезным проектным недостатком, а такие системы являются весьма распространенными. Североамериканская корпорация по обеспечению надежности электроэнергетических систем (NERC) опубликовала руководящие указания, на основе результатов демонстрации. Критики заявили, что наличие такого вида защиты генераторов, уже является распространенной практикой для генераторов, подключенных к высоковольтным электрическим системам, которые регулируются NERC. Критики также заявили, что эксперимент был проведен с нарочитой уязвимостью, или даже внимание специально было уделило этим уязвимостям для создания эффектной демонстрации. Организатор и другие участники категорически отрицали, что это правда.

Одна из целей демонстрации – сделать сенсационное заявление о серьезности угрозы, вызванной недостатками системы информационной безопасности. Организаторы считали, что руководство электроэнергетической компании не воспринимало эти угрозы достаточно серьезно. Они понимали, что многие энергетические компании предполагали, что такие уязвимости могут

[15] http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html
[16] https://www.selinc.com/WorkArea/DownloadAsset.aspx?id=6379

вызвать временные перебои в работе, но не могут привести к долгосрочному отключению. Если предположение организаторов об отношении энергетических компаний является верным, то демонстрация, возможно, была полезна. При том, что целесообразность проведения демонстрации может быть предметом спора, возникшее разногласие уменьшило эффективность демонстрации.

Прискорбно, что споры затмевают очень важный аспект информационной безопасности, а именно уязвимость доверенных систем. Предположение, что каждому полученному из сети сообщению можно доверять, и осуществлять управление на основе этого сообщения, является ошибкой проектирования. Такие ошибки могут привести к непредвиденным последствиям, результатом которых может быть все: от неправильного отображения данных на дисплее оператора до второстепенных отключений, либо, в худшем случае, повреждения или уничтожения критических активов. Разработчики системы защиты и управления должны принимать это во внимание перед выполнением управляющих воздействий.

### 4.6 Вынесенные уроки после нападения вирусам Stuxnet

#### 4.6.1 Введение

Атака вируса Stuxnet является единственной зарегистрированной сложно организованной кибератакой против промышленных систем управления, и эксперты в сфере информационной безопасности продолжают проводить тщательный анализ причинно-следственных связей. Тогда, как многие специалисты утверждали, что влияние Stuxnet было ограничено конечной целью вируса (заводом по обогащению топлива в Натанзе), такая оценка не является верной, если рассматривать не саму атаку, а используемые направления атаки. Те же направления атаки, некоторые из них даже с аналогичным программным кодом, могут быть эффективны против других целей в энергетическом секторе, например, кибератаки на электроэнергетическую сеть. Вопреки распространенному мнению, для таких подражательных атак не требуется потенциал национально-государственного масштаба. Stuxnet демонстрирует план, своего рода «золотой стандарт» для любой будущей кибератаки на промышленные системы управления. Этот раздел посвящен знаниям, полученным в ходе борьбы с этим вирусом, а также значениям для защиты киберпространства.

#### 4.6.2 Опытные злоумышленники нацелены не на IT системы, а на системы управления

Инцидент с вирусом Stuxnet четко обозначил то, что многие эксперты в области безопасности ICS предполагали долгое время: сложно организованная кибератака на промышленный объект лучше нацелится на систему управления, а не на IT систему. В случае с Stuxnet, IT система используется исключительно как средство распространения. Никто за пределами комплекса по обогащению топлива в Натанзе, у кого были инфицированные вирусом Stuxnet компьютерные системы, не испытал бы никаких проблем, кроме необходимости очистки компьютера. В качестве более серьезного побочного эффекта, «дроппер» показал насколько бесполезны современные антивирусные решения, когда речь идет о специально разработанных узко нацеленных вредоносных программах. Именно угроза такими средствами в энергетическом секторе должна вызывать беспокойство.

В отличие от обеспечения безопасности ICS до появления Stuxnet, вредоносное ПО не использовало целевые онлайн интерфейсы устройств управления для попыток повлиять на реальные технологические величины. Вместо этого, они использовали инженерный интерфейс для загрузки на устройства управления вредоносной логики управления, которая работала параллельно с настоящей логикой системы. Этого вполне достаточно для маломасштабных, работающих в режиме реального времени однозадачных систем. Триггеры, запрограммированные кодом для выполнения вредоносных операций, не требуют онлайн взаимодействия. Условия срабатывания частично заложены таймером (например, как срабатывание каждые 4 недели), а частично основаны на режиме технологического процесса.

Важным вопросом является то, что Stuxnet атаковал не только устройства управления производством, но и систему защиты. Сообщается, что этот вопрос все еще изучается компанией по информационной безопасности Langer Communications. Атака на систему защиты, которая

работает на базе контролеров Siemens 417 (вероятнее всего, резервная, или противоаварийная версия системы) является гораздо более сложной, чем известная атака на систему привода центрифуги, которая работала на основе контролеров Siemens 315, управляющие скоростью ротора центрифуги. Именно в случае с контролерами 417 вредоносный код переписывал отображение входного процесса в течение всей атаки. Таким образом, обеспечивая разрешенную логику управления (и HMI) предварительной записью поддельных входных данных. Несложно понять, как такое же направление атаки возможно в системе защиты в электроэнергетики, например, чтобы отключить цифровую систему защиты турбины.

Ни одно из слабых мест, на которое был нацелен Stuxnet, не квалифицируется как типичная IT уязвимость, как, например, потенциальное переполнение буфера. Все уязвимости представляют собой основные конструктивные недостатки, которые приходят вместе с преимуществами надежной эксплуатации. Это даже справедливо для хорошо известных IT уязвимостей, таких как способность исполнения кода с USB накопителя, не имея автоматического запуска. Тем не менее, в то время как Microsoft быстро зафиксировала IT уязвимости на уровне операционной системы, то же самое нельзя сказать об уязвимостях системы управления, где разработчикам потребовалось около двух лет, чтобы исправить некоторые, но не все из IT уязвимостей. Например, атака в целях внедрения вредоносного кода управления с помощью DLL все еще является действующей, так же как и атака через перезапись отображения входного процесса контролера. По сути, наиболее серьезные уязвимости, выявленные Stuxnet, можно обозначить как "характерные особенности", а не ошибки в программе. Для серьезных злоумышленников, особенности используемого продукта, безусловно, являются более привлекательными, чем ошибки и пропуски кодирования, поскольку существует высокая вероятность того, что они не будут исправлены до начала атаки.

### 4.6.3 Легкий способ преодоления физической изоляции

Было принято считать, что в энергетическом секторе наиболее значимые цели находились в безопасности, просто потому что они физически отделены друг от друга. Этот факт может быть заблуждением, но когда речь идет о физическом контроле доступа и доступе через интернет, не должно быть сомнений, что завод по обогащению топлива в Натзане является одним из наиболее защищенных производственных объектов на земле. Тем не менее, злоумышленникам удалось проникнуть на этот объект и внедрить вредоносный код в самые ответственные системы, которые, как и предположили в Langer Communications [27] даже не были подключены к локальной сети.

Единогласное решение исследователей состоит в том, что заражение произошло офлайн с помощью инфицированных ноутбуков подрядчиков, которые пользуются разрешенным доступом к системе. Предположительно, эти подрядчики не знали о вредоносной программе, которую доставили к цели. Эта атака проливает совершенно новый свет на возможность появления внутренней угрозы. При том, что более ранние виды угроз касаются недовольных штатных сотрудников, современная угроза находится в руках сотрудников, действующих из лучших побуждений, которые не имеют ни малейшего понятия, что их мобильные компьютеры и флэш-накопители являются каналом для внедрения уязвимости.

На опыте этой ситуации было извлечено несколько важных уроков. Очевидно, что в типичных процессах производства и передачи электроэнергии, где персонал (либо сотрудники или подрядчики) используют мобильные компьютеры и средства массовой информации для доступа и настройки критически важных систем, вероятность успеха подобной атаки будет весьма высока. К сожалению, даже спустя два года после нападения Stuxnet персонал работает без какого – либо соблюдения надлежащей политики в сфере информационной безопасности. Каждая крупная электростанция во время ежегодного отключения открывает свои двери для 1000 инженеров и подрядчиков по техническому обслуживанию, у которых осведомленность в сфере информационной безопасности обычно находится на минимальном уровне. Такая практика является рецептом катастрофы. Очевидно, что хитрый злоумышленник, вероятнее всего, выберет косвенный сценарий атаки, включающий разработчика в целях увеличения масштабов атаки. Изменить сотни настроек с помощью подставного подрядчика может быть намного проще, чем одну настройку с помощью прямой атаки. Другими словами, наивно восхвалять безопасность физически отделенных объектов, когда степень защиты от подрядчиков минимальна.

Еще один урок заключается в том, что устройства, программируемые в процессе использования,

являются самыми ответственными устройствами в плане информационной безопасности. Этот факт резко контрастирует с положением информационной безопасностью в обычных устройствах, которые, как правило, физически более доступны, используют ненадежные способы аутентификации, устаревшие операционные системы, и не имеют защиты от вредоносных программ. Столь очевидные уязвимые места сравнительно легко устраняются путем применения надлежащей политики в области безопасности. Применение вайтлистинга для предотвращения установки несанкционированного программного обеспечения является важным шагом вперед.

### 4.6.4 Проверки целостности данных недостаточно

Для более глубокого технического понимания, атака Stuxnet учит, что проверка целостности информации, которая обычно осуществляется с помощью системы безопасности, является недостаточной. В современных программных средствах для проверки целостности данных в логических устройствах управления и конфигурационных файлах используется циклический контроль избыточности, который хранится незащищенным в дисковых файлах. Хотя такие проверки целостности справляются с риском случайного преобразования данных из-за технических проблем, они не решают вопросы, связанные с вредоносными преобразованиями, так как злоумышленник может (и будет) легко манипулировать избытками информации для того, чтобы прийти к, казалось бы, бескомпромиссному, но вредоносному результату.

Непосредственное понимание заключается в том, что проверка целостности данных не обеспечивает защиту от вредоносных манипуляций, до тех пор, пока не будет дополнена проверкой подлинности данных. Это подтверждает факт того, что законной источник произвел первоначальный файл и избыточную информацию. Технологии, с помощью которых это делают, доступны в виде цифровых подписей и были в повседневном использовании в IT пространстве на протяжении многих лет. Потенциальному значению для использования в среде ICS применительно к производительности системы можно противопоставить тот факт, что такая проверка аутентификации требуется только во время загрузки (т.е. во время начала работы системы и после изменения конфигурации), но не во время выполнения программы. Регулирующей организации или самому производству нужно требовать надлежащие качества продукта от разработчика системы управления.

### 4.7 Последствия угроз для систем защиты и управления и систем SIPS

Главная проблема электроэнергетических компаний заключается в обеспечение техобслуживания сети, а также сведение к минимуму, насколько возможно, последствий неисправности в целях обеспечения надежности и качества электроэнергии для потребителей. В приложение N рассматриваются возможные последствия успешной кибератаке на систему защиты и управления или систему SIPS в электроэнергетических компаниях, что представляет интерес для инженера по эксплуатации систем защиты и управления.

## 5 Каковы практические решения для реализации информационной безопасности в системах защиты и управления

- Все практические решения требуют совместных усилий инженеров по эксплуатации систем защиты и управления и системного оператора и других специалистов со специальными навыками.

- Закрытые ворота, двери и шкафы с паролями для доступа к ИЭУ обеспечивают первую линию защиты для управления доступом.

- Защита от вредоносного программного обеспечения требует, чтобы все конечные точки контроля (смысла тоже не вижу) были специализированными устройствами, которые находятся под пристальным контролем и ограничены в выполнении разрешенных задач по поддержке, таких как управление конфигурацией.

- Политика безопасности должна обеспечивать соблюдение организационных директив, которые легко интегрируют сопровождение и поддержку безопасности в функциональные обязанности системы защиты и управления.

- Требуется защищать систему защиты и управления и компоненты с ограниченными ресурсами от киберугроз с помощью компенсирующих механизмов информационной безопасности (периметр защиты, демилитаризованные зоны и т.д.)

- В первую очередь вносить исправления в систему защиты и управления с целью устранения уязвимости, исходя из знаний о последствиях при использовании уже существующих систем безопасности, а также из влияния на производительность, надежность и бесперебойность работы системы защиты и управления. В первую очередь исправлять дефекты, которые могут привести к отказу срабатывания, и защищать систему от вредоносного программного обеспечения.

Более детальная информация о том, как осуществить данные решения, расположена в Приложении О.

# 6 Практические примеры нормальной работы системы для оценки влияния на систему информационной безопасности

## 6.1 Исходные параметры системы защиты и управления, необходимые при определении и анализе виртуальных инцидентов

### 6.1.1 Стратегия реагирования инженеров по эксплуатации систем защиты и управления на появление виртуальных угроз

Если инженера по эксплуатации системы защиты и управления попросить описать стратегию реагирования на появление угроз в системе информационной безопасности, то он, вероятнее всего, ответит следующее: "Каким образом киберугрозы отличаются от других нормальных рабочих вопросов, которые относятся к проектированию системы защиты и ее способов эксплуатации?" Ответ, как правило: "Нет никаких различий". Вне зависимости от того, что послужило причиной неисправности, система защиты автоматически действует на отключение, чтобы сохранить первичную систему, или постепенно выводит из работы отдельные устройства, чтобы дать инженерам достаточно времени для осуществления мер по устранению неисправности.

Отчет агентства ENISA на тему промышленной системы управления (ICS) для возможностей компьютерной системы реагировать на аварийную ситуацию (CERC) [28] или ICS-CERC, используется в настоящем докладе для описания возможностей, которые необходимо разработать экспертной группе по вопросам компьютерной безопасности в сети (CERT) для предоставления услуг по защите ICS и сетей ICS. Несмотря на то, что этот отчет об ICS, в нем размещено много полезных сведений о системе защиты и управления.

### 6.1.2 Реакция на неисправность в режиме реального времени

На рисунке 2 показан общий обзор реакции инженеров по эксплуатации системы защиты и управления на появление угроз системы информационной безопасности. В режиме реального времени (около четверти периода) система защиты получает значение величин, связанных с

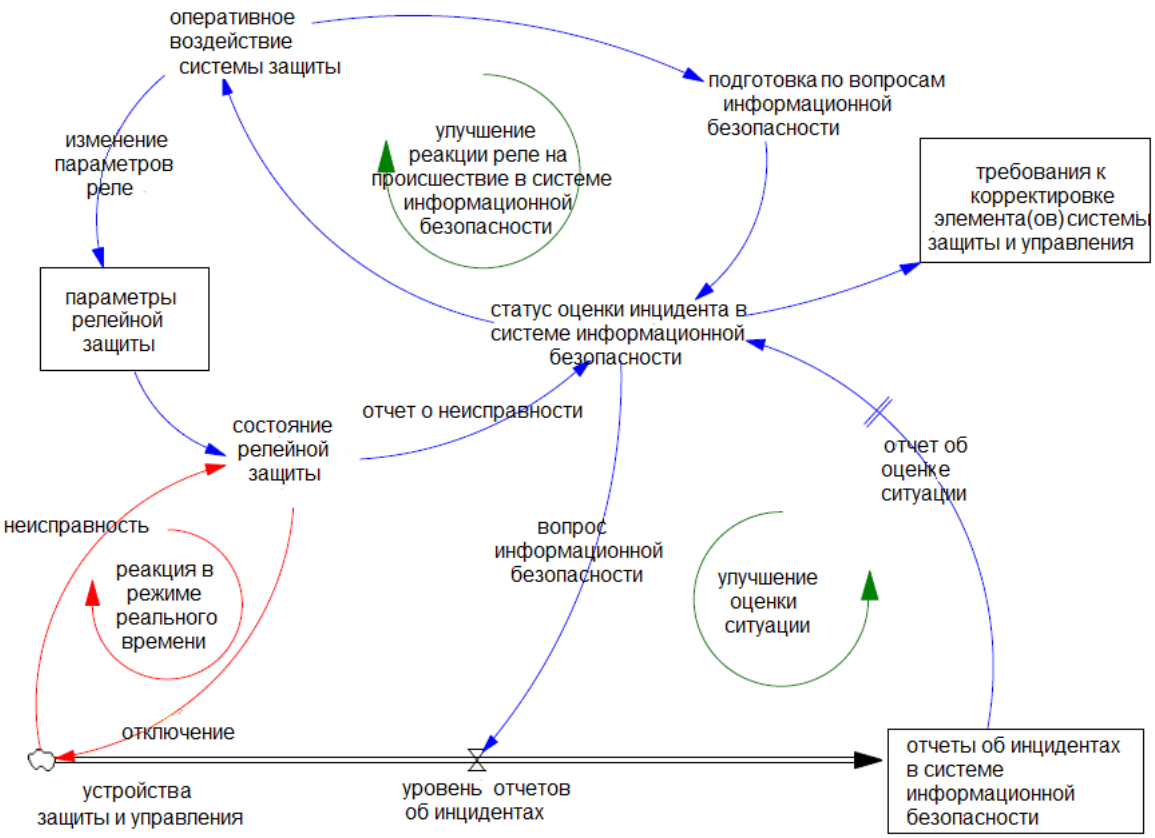



**Рисунок 2 Реакция инженеров по эксплуатации системы защиты и управления на виртуальную неисправность**

неисправностью, и, на основании настроек, реле изменяет свое состояние, что приводит к команде на отключение выбранных выключателей. Проект итогового отчета рабочей группы СИГРЭ B5. 31 [29, 30] описывает способы управления параметрами реле во время срока службы. Полное понимание того, как осуществляется управление параметрами, имеет значение при реакции на появление киберугрозы.

ПРИМЕЧАНИЕ: На рисунке 2, а далее на рисунке 3, используются обозначения для моделирования системной динамики в программе Vensim [31]. Стерман [32] предусматривает предметное обсуждение моделирования динамики производства. Чтобы понять детали обозначений, читателям рекомендуется получить бесплатную версию Vensim PLE для использования в образовательных целях. В этой технической брошюре измененные обозначения Vensim предоставляют более привычную терминологию для инженеров системы защиты и управления. Терминология Vensim приведена в квадратных скобках "[]" для того, чтобы обеспечить соответствие между терминологией, относящейся к системе защиты и управления, и терминологией программы Vensim. Краткое изложение обозначений представлено в следующем списке.

- Стрелки обозначают взаимодействие между двумя параметрами, ситуациями или условиями в контуре причинно-следственных связей. Каждое звено в диаграмме взаимодействия имеет конкретное [рабочее] значение. Стрелка, идущая от A к B, указывает на то, что A является причиной B. Диаграммы взаимодействия могут быть очень полезны в объяснении понятий и передаче данных между структурами.

- Количество или приведенный массив данных [накопитель] и диаграммы интенсивности [поток] являются способами представления структуры в системе с более подробной информацией, чем показано на диаграмме взаимодействия.

- Накопители представлены в виде прямоугольников (предположительные хранилища данных, где находятся содержащиеся в данных сведения; например, набор действующих требований, группа действующих параметров настройки реле, отчеты об инцидентах.)

- Накопители имеют основополагающее значение для формирования поведения системы; интенсивность потока является причиной изменений, происходящих в накопителе.

- Использование накопителей и диаграмм интенсивности является первым шагом в построении имитационной модели, поскольку они помогают определить типы переменных, которые важны для изменения поведения системы.
- Притоки представлены в виде трубок (стрелок), указывающих на (дополняющих) накопитель.

- Оттоки представлены в виде трубок исходящих (вычитающих) из накопителя.

- Клапаны контролируют скорость изменения потока, направленного в накопитель.

- Облака представляют собой источники и стоки информации, которой обмениваются два объекта.

- Источник представляет собой накопитель, где изменения в массиве данных возникают за пределами модели.

- Стоки представляют собой накопитель, куда за границу модели направляются изменения в массиве данных.

- Предполагается, что источники и стоки имеют неограниченную емкость и не могут ограничивать изменения, происходящие в массивах данных, которые они питают.

- Кнопка «Variable» создает переменные (т.е., константы, вспомогательные функции и т.д.).

- Кнопка «Box variable» создает переменные, заключенные в форму прямоугольника (используется для создания накопителей).

### 6.1.3 Оценка инцидентов в системе информационной безопасности

Мы предполагаем, что отчет о неисправности с целью проведения ретроспективного анализа должен включать в себя все вспомогательные данные. Ретроспективный анализ включает в себя оценку инцидентов в системе информационной безопасности. На рисунке 2 подчёркивается необходимость проведения надлежащей подготовки инженеров по вопросам инцидентов в системе информационной безопасности. Данная подготовка, в сочетании с обязанностями инженеров системы защиты и управления, является необходимым условием, чтобы определить, относилась ли неисправность к системе информационной безопасности. Если относилась, то описывающий проблему отчет отправляется в соответствующий отдел, который занимается инцидентами в сфере информационной безопасности для связи данного инцидента с другими. В конечном счете, отдел, занимающийся инцидентами, отправляет отчет об оценке ситуации в электроэнергетическую компанию (EPU) и далее в инженерную организацию системы защиты и управления.

Некоторые организации собирают и сопоставляют отчеты об инцидентах. Трудность обмена информацией между этими организациями приводит к задержкам (показано символом ||) в формировании полезных отчетов по оценке ситуации. Для особо важных приложений системы защиты и управления инженерам в электроэнергетических компаниях придется решать, как уменьшить вероятность возникновения киберугрозы без помощи отчетов об оценках ситуаций из координационного центра.

### 6.1.4 Необходимость надлежащей подготовки инженеров системы защиты и управления по вопросам информационной безопасности

Эрнандес и др., позаимствовали теорию о лестнице узнаваемости из нефтехимической промышленности. Данная теория обеспечивает прекрасную основу для подготовки инженеров по вопросам информационной безопасности [33, 34].

**Восприятие**: Способность инженера по эксплуатации системы защиты и управления распознавать или обнаруживать показатели атак на систему информационной безопасности.

**Осознание**: Способность инженера по эксплуатации системы защиты и управления понимать

значение данных показателей поведения системы с помощью устройств защиты.

**Прогнозирование**: Способность инженера использовать показатели неисправности, чтобы предсказать или предвидеть, какие отклонения от заранее заданной реакции системы защиты нуждаются во внимании.

В библиографической ссылке также находятся модели системной динамики, показывающей отношения между системными недостатками и ведущими кризисными показателями, а также модель, связывающая принятую процедуру с показателями и системные недостатками.

### 6.1.5 Важные исправления компонентов в системе защиты и управления

Вик, Гонсалес, Липсон и Шимил представили всеобъемлющий документ для общества системной динамики в 2004 году под названием «Dynamics of vulnerability – modeling the lifecycle of software vulnerabilities» [35]. Мы использовали обсуждение в цитируемой работе, чтобы изучить какие исправления в объекте системы защиты и управления нужно осуществлять в первую очередь.

На рисунке 3 показана некоторая динамика, которая демонстрирует, что инженеры эксплуатации системы защиты и управления выполняют настройку с целью корректировки уязвимых компонентов системы защиты и управления. Эта модель системной динамики является хорошей отправной точкой для инженеров по эксплуатации систем защиты и управления, т.к. она оправдывает ускорение работы при критическом исправлении ошибок и при введении исправленных компонентов. Цель состоит в том, чтобы уменьшить число уязвимых компонентов системы защиты и управления и увеличить число защищенных.
Модель демонстрирует четыре балансирующие петли системной динамики[17].

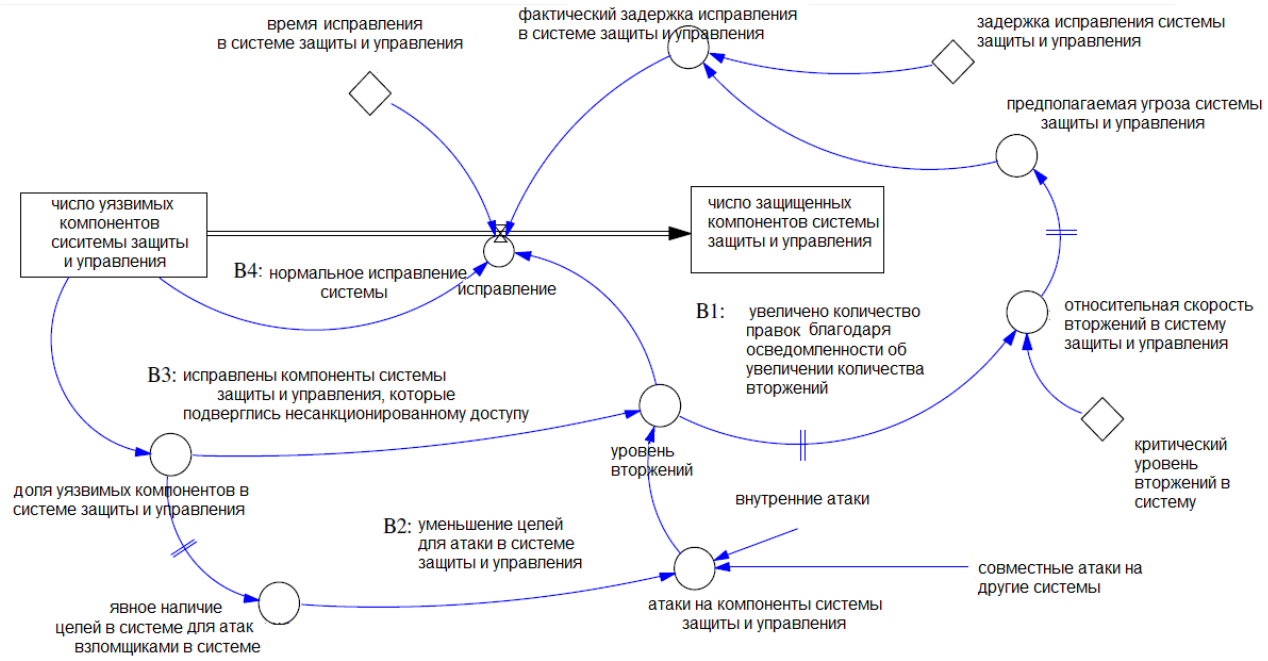



**Рисунок 3 Срочное исправление компонентов в системе защиты и управления**

B1: показывает, что количество внесенных исправлений возрастает из-за большего числа несанкционированных вторжений. Осознание данной зависимости оказывает сильное влияние на активное участие инженеров в оценке инцидента в системе информационной

[17] На рисунке 3 не рассматривается возможность внедрения дополнительных уязвимых компонентов в систему при внесении исправлений. Для решения вопроса, рекомендуется провести тщательное тестирование в лаборатории контроля качества электроэнергетической компании – см. Приложение F.

безопасности. Данная оценка показана на рисунке 2.

B2: показывает, что исправления уменьшают количество целей для атаки взломщиками, т.к. из-за внедрения все большего количества исправленных компонентов, количество доступных целей будет снижаться. Это оказывает необратимое воздействие на уровень вторжений, но с определенной задержкой (обозначается || на стрелках), а также влияет на количество кибератак, т.к. злоумышленникам просто не удастся найти цели для атаки.

B3: показывает, что внесение исправлений в уязвимые компоненты системы защиты и управления также снижает уровень вторжения по сравнению с нормальным исправлением системы, которое показано в контуре B4.

B4: нормальное внесение правок в систему защиты и управления.

Инженеры по эксплуатации системы защиты и управления могут делать любые попытки минимизировать время задержек, которые показаны на рисунке 3.

- База данных системы защиты и управления (для управления конфигурацией) включает в себя актуальный перечень уязвимых компонентов системы для несанкционированного доступа и управления пользованием. На основе анализа рисков и потенциальных последствий, признак уязвимости компонентов воспринимается как цель для частого мониторинга.

- Внутренняя атака (осуществимая сотрудниками компании и разработчиками системы защиты и управления) на компоненты системы и нападения на компоненты, не относящиеся к системе защиты и управления, являются основными факторами, определяющим уровень кибератак. Необходимо автоматизировать процесс контроля доступа и использовать журналы контроля, чтобы свести к минимуму время, необходимое для определения, превышен ли порог по уровню вторжений.

- Если уровень вторжений в систему превышает порог, необходимо начать своевременные меры по управлению системой в целях смягчения последствий от предполагаемой угрозы.

### 6.2 Использование переносных носителей техническим персоналом – см. наглядный пример в Приложении L

#### 6.2.1 Введение

Большинство инженеров и техников по эксплуатации системы защиты и управления, которые не специализируются в области информационной безопасности, часто ставят под сомнение вероятность появления угроз для системы информационной безопасности. Конечно, трудно представить, что для небольших энергетических компаний, будет организовано согласованное нападение террористической группы или иностранного правительства. В свою очередь, некоторые кибератаки имеет высокую вероятность возникновения. Распространение вредоносных программ (вирусов, сетевых червей и т.д.), безусловно, одно из часто встречающихся событий в сфере информационной безопасности для любого субъекта.

Инженеры по эксплуатации систем защиты и управления и руководящий состав предприятия должны серьезно относиться к нападению вредоносных программ, т.к. данные нападения являются спонтанными, заранее не запланированы и не имеют конкретной цели. Лучшие представители технического персонала, имея самые хорошие намерения, могут с таким же успехом сами внедрить вредоносные программы в систему защиты, на которую не были нацелены. Фактически данный вопрос является проблемным, потому что в отличие от других видов кибератак, вредоносные программы не имеют конкретной цели.

Например, вирус, заражающий SQL-сервер с целью вывести его из строя, может легко оказаться в HMI подстанции. Этот вирус не был нацелен на сферу применения HMI, или даже на более конкретный объект. Тем не менее, результат ставит под угрозу систему защиты и управления.

С учетом вышесказанного, важно проанализировать все места проникновения вредоносного ПО,

чтобы исключить вероятность его появления в местах внедрения. Некоторые места проникновения остаются открытыми для оперативного или технического обслуживания, в таком случае важно обеспечить безопасность данных точек.

Использование переносных носителей, таких как USB-накопители, безусловно, является одним из наиболее вероятных способов внедрения вредоносного ПО в систему защиты и управления. Чтобы продемонстрировать вопросы обеспечения безопасности в системе и важность мер по ослаблению последствий, в этом разделе основное внимание будет уделено именно этому способу заражения.

### 6.2.2 Необходимые функции обеспечения безопасности на мобильных устройствах

Мобильные устройства, которые используются для управления файлами конфигурации систем защиты и управления, а также файлами настройки, должны быть основными объектами оценки. Для обеспечения безопасного выполнения программ на мобильных устройствах, используемых удаленно или локально уполномоченным для доступа к системе защиты персоналом, устройства должны предоставлять следующие возможности:

а) Возможность ограничения функционирования программ в режиме запуска модуля системы ПО на мобильном устройстве в полной изоляции от остального кода, чтобы обеспечить конфиденциальность и целостность кода модуля и данных за время функционирования программы.

б) Безопасное хранение данных на мобильном устройстве в целях обеспечения конфиденциальности, целостности и/или свежести хранимых данных программного модуля (при выключенном состоянии мобильного устройства, а также при определенных условиях, исходя из того, какое ПО было загружено). Для исполнения этой функции требуется корень доверия для хранения (RTS). RTS может загрузить достаточно большой механизм безопасного хранения с использованием герметичного хранения. Для шифрования данных, а также для защиты подлинности данных и прикреплённых метаданных примитивная герметичная система хранения должна использовать защищенный с помощью RTS ключ. Метаданные включают в себя политику контроля доступа, для которой установленный код запрашивает дешифрование, а также данные о том, какой модуль программного обеспечения изолирует данные в первую очередь. Герметичные данные (зашифрованный текст) могут быть сохранены на незащищенных устройствах хранения.

c) Удаленная аттестация позволяет удаленным сторонам убедиться, что конкретное сообщение пришло от конкретного программного модуля мобильного устройства. Для того, чтобы аттестация имела смысл, она должна аттестована всей достоверной компьютерной базой (TCB) данного приложения. Механизмы аттестации обычно используют закрытый ключ, который доступен только небольшой TCB и находятся в защищенном хранилище. Паспорт, выданный доверенной стороной, например, производителем устройства, подтверждает, что соответствующий открытый ключ принадлежит мобильному устройству.

d) Защищенное выделение ресурсов - это механизм, который передает данные в конкретный модуль программного обеспечения, работающий на конкретном мобильном устройстве, защищая при этом конфиденциальность и целостность этих данных. Данный механизм полезен при перемещении данных конфигурации системы защиты и управления и данных настроек между устройствами пользователя. Один из способов построить безопасный механизм выделения ресурсов это использовать удаленную аттестацию с целью подтверждения, что открытый ключ шифрования принадлежит конкретному модулю ПО, установленном на конкретном мобильном устройстве. Отправитель может затем использовать этот ключ для защиты данных, отправляемых в модуль целевого программного обеспечения на целевое интеллектуальное электронное устройство (IED) системы защиты и управления.

e) Защищенный канал защищает достоверность, конфиденциальность и доступность связи между модулем программного обеспечения и внешним устройством (например, клавиатурой или сенсорным экраном). При использовании совместно с портативными HMI устройствами, это свойство позволяет пользователю точно определить работающее в данный момент

приложение. При полной поддержке защищенного канала вредоносные приложения, которые пытаются подменить существующие приложения путем создания идентичных пользовательских интерфейсов, предположительно, будут неэффективными.

### 6.2.3 Инструмент для анализа вариантов смягчения последствий

Для анализа различных вариантов смягчения последствий используется язык моделирования информационной безопасности (CySeMoL), который является программным инструментом для анализа системы информационной безопасности предприятий. В этой статье приводится краткое описание концепции данного инструмента. Более подробное описание будет опубликовано в [36].

CySeMoL охватывает целый ряд IT-атак, таких как: внедрение кода, флуд атаки, получение нелегальных полномочий и психологическая атака. Основная цель CySeMoL заключается в том, чтобы позволить пользователям создавать модели своих собственных архитектур и рассчитывать вероятность появления различных атак. От пользователя не требуется проводить экспертизу системы безопасности, так как модель включает в себя теорию о том, как атрибуты в модели объекта влияют друг на друга. Другими словами, пользователи должны только моделировать архитектуру и свойства системы.

Элементы в CySeMoL включают в себя различные IT-компоненты, такие как: операционная система (например, Windows XP); межсетевой экран; программа по повышению информированности о вопросах безопасности (например, обучение в сфере IT безопасности); управление зонами (то есть поддержка безопасности сетевых зон); а также персонал (пользователь). Каждый элемент системы имеет набор атрибутов, которые могут быть как угрозами, так и средствами защиты. Между этими атрибутами существует взаимосвязь. Например, пользовательские пароли могут подвергнуться воздействию психологической атаки. Тем не менее, вероятность успешной атаки зависит от того, прошел ли пользователь подготовку по вопросам безопасности или нет. Каждый атрибут в CySeMoL может иметь значение *истина* или *ложь*, которое отображает либо вероятность успешной атаки на систему, либо вероятность эффективной меры защиты.

Смоделированная система объединённой рабочей группы находится в Приложении L. Она использует типичную архитектуру электрической подстанции – см. результаты опроса JWG за середину 2012 г. в приложении D. Следующие основные положения описывают варианты стандартного моделирования.

- Управляемая подстанция через локальную сеть соединяет устройства защиты и управления.
- Точка доступа к корпоративной сети защищена межсетевым экраном.
- Контроль локальной сети использует комбинацию протоколов приложений, часть которых зашифрована (например, протоколами RDP или SSH), а часть не зашифрована (Telnet).
- Устройство HMI является персональным компьютером, который не является частью программы управления исправлениями.
- Пользователи устройств защиты и управления имеют одинаковые учетные данные (имя пользователя и пароль) для каждого устройства.
- Удаленный доступ осуществляется через шлюз.
- Сотрудники имеют минимальную подготовку по вопросам безопасности
- Модель управления локальной сетью включает в себя типичные IED. (HMI, RTU, реле защиты, выключатели и т.д.)

С помощью описанной выше модели, вероятность успеха кибератаки через USB-порты составляет 56%. В таблице 3 показаны различные типы изменений в исходной модели и их влияние на

вероятность успеха кибератаки.

**Таблица 3 Вероятность успеха кибератаки через USB-порт**

| Изменения в модели | Вероятность успеха кибератаки |
|---|---|
| Стандартное условие | 56% |
| Запрет использования USB-накопителя | 0% |

Результаты показывают, что при более или менее простых изменениях в политике информационной безопасности энергетического объекта, как, например, ознакомительный курс по безопасности для персонала, вероятность успеха информационной атаки может значительно уменьшиться. Такая мера технического контроля, как использование антивируса, дает хорошие результаты, но добавляет рабочую нагрузку техникам, и никто не может гарантировать, что перед использованием USB-носителя будет проводиться его сканирование.

Запрет использования переносных носителей в системе защиты и управления является более радикальной мерой. Например, для передачи данных можно использовать компакт-диск вместо USB или передавать данные по сети через проверенный источник загрузки. Данные мероприятия позволят значительно снизить риск распространения вредоносных программ, но в равной степени бдлш
Существует широкий спектр мер безопасности, которые могут снизить риск распространения вредоносных программ с помощью портативных устройств. Помимо упомянутых выше, другие меры контроля безопасности могут включать в себя: программу управления исправлениями, меры укрепления хоста, антивирус обеспечиваемый хостом, вайтлистинг, аккаунт с ограничением полномочий и т.д. Предприятия могут использовать одно или несколько мер безопасности. В конечном счете, можно подчеркнуть два важных момента:

1. первоначальный риск, составляющий 56% , является неприемлемым, и
2. контроль безопасности оказывает значительное влияние на вероятность успеха кибератак.

Инженеры по эксплуатации системы защиты и управления должны применять меры по управлению системой безопасности как часть процедуры проектирования и ввода в эксплуатацию с тем, чтобы снизить риск распространения вредоносных программ. Как уже говорилось выше, вероятность распространения вредоносных программ очень высока.
Одним словом, типичная модель, которой пользуется большинство энергетических компаний, как отмечено в исследовании, не является приемлемой с точки зрения риска, а также работы, необходимой инженерам для применения мер безопасности в целях снижения данного риска. При отсутствии значительных финансовых ресурсов для внедрения сложных механизмов, компания может использовать процедурные и предупредительные средства управления системой безопасности, описанные в данном пункте. Они могут оказать значительное влияние на вероятность успеха кибератак такого рода.

### 6.3 Управление на лицевой панели

#### 6.3.1 Настройка управления на лицевой панели

На некоторых старых реле защиты имеются кнопки для настройки. Для этих реле не может быть никакого контроля доступа, кроме закрытых дверей в помещении. Для изменения настроек новые защитные реле имеют входной порт для подключения ноутбука. Все изменения для реле защиты загружаются с ноутбука, и для осуществления данных изменений требуется пароль. Управление доступом к системе для внесения изменений разрешено выполнять только уполномоченному персоналу. Пункт 6.2 выявляет проблемы и способы решения многих из этих проблем. В пункте 6.2 обсуждался вопрос, касающийся USB накопителей, и незащищенный ноутбук имеет такие же проблемы. Проведение ознакомительного курса по безопасности для персонала и использование антивирусных ПО являются лучшими решениями.

### 6.3.2 Тестирование вводов на лицевой панели

Все реле защиты имеют на передней панели контрольные точки ввода. Расположение и конструктивное оформление варьируется в зависимости от завода-изготовителя. Большинство защитных реле имеют встроенные контрольные вводы, но большая часть энергетических компаний также добавляют отдельные вводы, как правило, на панель, содержащую защитное реле. Обычно тестирование релейной защиты проходит с определённым интервалом времени (частота проведения тестирования определяется энергетической компанией). После задания настроек, тесты реле показывают, корректно ли заданы установки. Устройства для тестирования подключаются к испытательным вводам, подается определенная величина тока и напряжения и определяется, сработает или не сработает при них реле. Как только получен выходной сигнал срабатывания, происходит размыкание в цепи с автоматическим выключателем.

Это одна из причин физической защиты реле. Любой человек, обладающий знаниями и намерениями способен вызвать срабатывание реле по данному методу. В настоящее время физическая защита (т.е. закрытие дверей и ворот в помещение) является единственным известным способом защиты от агрессивных действий со стороны.

## 6.4 Управление безопасностью HMI

### 6.4.1 Введение в управление безопасностью HMI

Ни возможность подключения HMI на базе ПК, ни его операционная система не должны быть основанием считать HMI надежным и упускать из виду вопрос информационной безопасности. Очень часто инженеры систем защиты и управления предполагают, что, поскольку HMI не доступен из корпоративной сети или из интернета, в мерах информационной безопасности нет необходимости. Другим распространенным предположением является то, что Linux или ОС собственной разработки редко становятся объектами информационных атак или вредоносных программ.

Хотя предыдущие заявления не являются неверными, они и не совсем правильны. Эти два предположения используются при оценке риска для выбора применяемого режима управления информационной безопасностью. Это может дать инженерам систем защиты и управления основания полагать, что системы, основанные на этих ОС менее подвержены риску и поэтому не требуют серьезной, или какой-либо, защиты. Подобное рассуждение фактически увеличивают риск, потому что оно оставляет потенциальную точку доступа, которая в конечном итоге будет атакована.

Хорошо известно, что, чем больше уровень безопасности, тем меньше эксплуатационная гибкость. Когда остановится, если речь идет об программных компонентах системы информационной безопасности, которые относятся к цели компонентов систем защиты и управления. В случае HMI подстанций электроэнергетических компаний, существует тенденция к статической конфигурации и среде. Требования эксплуатационной гибкости не должны быть большой проблемой для инженеров систем защиты и управления. Главным фактором уровня безопасности должен быть риск, связанный с HMI. Например, HMI, способному контролировать всю подстанцию, должно уделяться больше внимания, чем HMI, специализированному на подсистеме. Сотрудники по информационной безопасности и инженеры систем защиты и управления должны оценить необходимость в эксплуатационной гибкости и решать совместно, потому что их знания и приоритеты слишком часто различаются.

При определении уровня эксплуатационной гибкости, приемлемого риска, безопасности и управления принимается решение, выбираются и применяются соответствующие средства управления информационной безопасности. Независимо от уровня безопасности, для защиты доменов применяется, по крайней мере, одно из средств контроля безопасности, которые описываются в следующих подразделах.

### 6.4.2 Предотвращение появления вредоносных программ

Защитой от вредоносных программ в системах защиты и управления, в которых отсутствует

внешнее подключение, часто пренебрегают. Если на конечном устройстве не существует никаких средств предотвращения появления вредоносных программ, то нет элемента безопасности, который защищает HMI от повреждений данных локальными действиями. Как минимум блокировка в электронной или физической части защиты предотвращает внешние атаки. Когда дело доходит до локально установленных вредоносных программ (например, USB - накопитель), только конечные устройства контроля безопасности защищают HMI. Кроме того, в отличие от внешних атак, часто установка вредоносной программы происходит на местном уровне людьми, которые не знают, что они заражают устройство.

Надежная политика по предотвращению появления вредоносных программ должна включать в себя сочетание мер управления системой безопасности, которые представлены в таблице 4.

**Таблица 4 Руководящие принципы контроля безопасности против появления вредоносных программ**

| Механизм защиты | Рекомендации по реализации |
|---|---|
| Обновляемые антивирусы | Обновление антивируса необходимо осуществлять по графику. Если не осуществлять техническое обслуживание, создастся ложное представление о безопасности. |
| | Когда автоматическое обновление или удаленное обновление не поддерживается, следует использовать с осторожностью обновление вручную, так как частота обновления, вероятно, будет слишком велика. Кроме того, слишком много действий на HMI увеличивают риск человеческих ошибок. |
| Серверные системы предотвращения вторжений (IPS)/ обнаружения вторжений(IDS). | IPS/IDS обычно предлагают возможность остановить ненормальную деятельность или оповестить о ней. Необходимо использовать функции блокировки с осторожностью, так как ошибочное срабатывание является обычным явлением. Для особо важных систем рекомендуются включение оповещений. |
| Межсетевой экран узлов (HBFW) для входящего и исходящего трафика | HBFW должен блокировать весь трафик по умолчанию. Необходимо указывать приемлемый трафик. |
| | В зависимости от требуемого уровня конфиденциальности, использование межсетевого экрана для входящего трафика может быть приемлемо. (Межсетевой экран Windows XP является экраном только для входящего трафика). |
| Меры усиления защиты | Отключают автозапуск для внешних носителей. |
| Вайтлистинг | В статической среде подобно подстанциям электроэнергетических компаний, вайтлистинг может быть очень эффективным в предотвращении заражения вредоносным вирусом. Основным недостатком является эксплуатационная гибкость вайтлистинга. Установив однажды, администратор должен перенастроить вайтлистинг для каждой установки нового приложения, обновления и т.д. |

### 6.4.3 Идентификация и опознавание

Для компьютера, подсоединенного к домену[18], легче реализовать контроль идентификации и опознавание, так как опознавание происходит по сети к серверу управления (например, активный каталог). Общие учетные записи используются для неприсоединённых к домену компьютеров.

HMI, скорее всего, не будут присоединенным к домену компьютерами с некоторой ролевой учетной записью. Такой как, например, учетная запись администратора для конфигурации компьютера, аккаунт по обслуживание программного обеспечения и утилит, необходимых для выполнения задачи по техническому обслуживанию систем защиты и управления и учетная запись оператора по управлению процессом.

[18] Если пользователи возьмут домой компьютер, который является частью домена на работе, и присоединят компьютер к домашней группе [Microsoft Windows], они не смогут делиться любыми файлами с рабочего компьютера с компьютерами в домашней группе. Эта функция безопасности предотвращает непреднамеренное распространение конфиденциальной информации другим пользователям домашней группы.

Как минимум пароль защищает доступ к этим учетным записям. Тем не менее, в учетной записи оператора использовать пароли необходимо с осторожностью, поскольку ввод пароля в критических ситуациях может задержать выполнение действий оператором для управления подстанцией. В таких случаях, аналогичный подход заключается в использовании сильного физического контроля безопасности.

Хотя, намного дороже использовать физический маркер и биометрическое опознавание. Оценка риска может не оправдать инвестиции.

### 6.4.4 Безопасность и административная конфигурация

Для всех HMI системы защиты и управления включают основное обеспечение безопасности для административной конфигурации. В связи с тем, что большинство операционных систем являются объектами атаки, для HMI систем защиты и управления настройки по умолчанию редко подходят.

Конфигурация должна включать в себя действия, описанные в таблице 5.

**Таблица 5 Руководящие принципы по управлению административной безопасностью**

| Действия внутренней проверки | Основополагающие принципы реализации |
|---|---|
| Проверка сети и местных служб | Проверка всех служб по умолчанию. |
| | Закрытие каждой неиспользуемой программы(например, Windows Messenger). |
| Проверка конфигурации параметров безопасности | Соответствие с политикой локальной настройки |
| Проверка активных открытых портов | Закрытие всех ненужные портов и включение блокировки с помощью серверного межсетевого экрана. |
| Проверка разрешений доступа к файлу | Проверка каждый файл для разрешения доступа, например, с помощью списка управления доступом (список контроля доступа). |
| Проверка разрешения на расширение программного обеспечения и файлов | Методы ограничения использования программ являются обычным способом выполнения такого контроля. |
| Ведение журнала и контроль отчетности | Избежание настроек журнала по умолчанию (например, неудачные попытки входа в систему). |

Периодический критический просмотр конфигурации безопасности HMI необходим с целью проверки того, что предыдущие решения конфигурации все еще пригодны. Для электроэнергетического объекта с большим количеством HMI рекомендуется использовать шаблоны и базовую версию, чтобы убедится, что это не присоединенный к домену компьютер. Периодическая проверка использует базовую версию в качестве исходных данных. Также может быть выполнен некоторый неавтоматический контроль отчетности на месте для того, чтобы проверить внедрение базовой версии.

Некоторые организации для начала предлагают базовую версию. Например, НИСТ (http://usgcb.nist.gov/) предлагает различные базовые версии для различных версий Windows. Некоторые настройки могут не подходить для конкретного приложения, но базовая версия подойдет для начала работы.

## 6.5 Обеспечение соблюдения организационной и управленческой политики в области информационной безопасности

### 6.5.1 Изменения исполнительных нормативов

Регулирующие органы страны, в которой находятся электроэнергетические компании, издают организационно-распорядительные документы. Электроэнергетические компании затем пишут технические правила, которые соответствуют данным документам. В большинстве случаев электроэнергетическим компаниям придется получить внутренний регламент, одобренный регулирующим проверяющим органом, что они соответствуют требованиям, изложенным в приказах. Электроэнергетические компании самостоятельно осуществляют контроль, за исключением редких проверок регулирующего органа.

Это приводит к широко распространенным различиям между электроэнергетическими компаниями, так как различные регулирующие органы устанавливают разные требования и различные электроэнергетические компании интерпретируют требования по-разному.

### 6.5.2 Доступ сторонних организаций к цифровой системе автоматизации подстанции

Некоторые электроэнергетические компании используют персонал сторонних организаций для обслуживания и модернизации их цифровой системы автоматизации подстанции (ЦСАП). Эти сотрудники нуждаются в подготовке по вопросам информационной безопасности в соответствие с требованиями, предъявляемыми к информационной безопасности и к существующей политике в области данной безопасности в данной электроэнергетической компании. Политика электроэнергетических компаний требует проверки персонала сторонних организаций по необходимым уровням безопасности для доступа к ЦСАП. Электроэнергетические компании должны иметь нормы проверки персонала, относящийся к лицам сторонних организаций перед приходом на подстанцию, чтобы убедиться, что данные лица отвечают всем требованиям для выполнения работ на подстанции.

### 6.5.3 Обслуживающий персонал

Различному обслуживающему персоналу необходима подготовка по вопросам, относящимся к системе информационной безопасности и политики электроэнергетической компании. Уникальная система паролей для обслуживающего персонала отражает их уровень доступа к какой-либо конкретной части ЦСАП. База данных ролевого управления доступом должна отражать их уровень доступа к какой-либо конкретной части ЦСАП.

# Приложение А

# Определение терминов и сокращений

## А.1 Определения терминов

**А.1.1**
**активы (системы защиты и управления)**
любые ресурсы системы защиты и управления и сетевые ресурсы, которые имеют ценность для организации систем защиты и управления и необходимы для достижения целей этих огранизаций.

ПРИМЕЧАНИЕ В данной технической брошюре проводится различие между критическими и некритическими активами.

**А.1.2**
**метод обеспечения**
все запланированные и систематические мероприятия, осуществляемые в рамках системы защиты и управления, которые можно продемонстрировать с целью обеспечения уверенности в том, что продукт или услуга будет соответствовать требованиям к ожидаемой защите информационной безопасности [модифицируется на основании ISO 15531-1: 2004]

**А.1.3**
**атака**
попытка поставить под угрозу информационную систему защиты и управления, которая осуществляется со злонамеренными целями

**А.1.4**
**доступность**
свойство, позволяющее в нужное время выполнять ожидаемое обслуживание в соответствии с ожидаемыми условиями использования защиты и управления

**А.1.5**
**передовой практический метод**
главный метод или инновационная практика, который способствует улучшению производительности организации, как правило, электроэнергетическими компаниями и аналогичными организациями признается в качестве "лучшего"

ПРИМЕЧАНИЕ 1 Членство в подобной организации является вопросом местного характера, который определяется политикой безопасности и внутренним регламентом электроэнергетических компаний.

ПРИМЕЧАНИЕ 2 Членство в подобной организации должно включать членство всей группы заинтересованных лиц, имеющих интерес к защите активов систем защиты и управления.

**А.1.6**
**черный список**
список или реестр лиц, которым по той или иной причине, отказывают в предоставлении конкретной привилегии, обслуживания, мобильности, доступа или идентификации.

**А.1.7**
**центр сертификации**
организация, которая выдает цифровые сертификаты

ПРИМЕЧАНИЕ Цифровой сертификат удостоверяет право собственности на открытый ключ названного субъекта сертификата. Это позволяет другим (доверяющим сторонам) полагаться на подписи или утверждения, сделанные закрытым ключом, соответствующим сертифицированному открытому ключу. В этой модели доверительных отношений, центр сертификации является доверенной сторонней организацией (доверенной как субъектом (владельцем) сертификата, так и организацией, которая полагается на сертификат). Центры сертификации являются показателями для многих инфраструктур с открытыми ключами.

**А.1.8**
**сторона клиента**
Операции, выполняемые клиентом в отношениях клиент-сервер в компьютерной сети

ПРИМЕЧАНИЕ 1 конфигурации систем защиты и управления или инструмент технического обслуживания приложений, который работает на локальном компьютере электроэнергетической компании, рабочей станции или на собственном устройстве сотрудника и соединяется с сервером (с компонентом систем защиты и управления или IT-компонентом сети) по мере необходимости.

ПРИМЕЧАНИЕ 2 действиям со стороны клиента необходим доступ к информации или функциональным возможностям ПО, которые доступны клиенту, но не серверу, так как пользователь должен принимать во внимание информацию или предоставлять ее, а также учитывать, что серверу может не хватать вычислительной мощности для своевременного выполнения операций для всех клиентов, которых он обслуживает. Кроме того, если клиентом произведены операции без отправки данных по сети, то это может занять меньше времени и меньше загрузить сеть. А также данные действия влекут за собой меньшую угрозу безопасности.

**А.1.9**
**настройка конфигурации**
набор значений в защитном реле, которые обеспечивают пользователю возможность применять ряд различных параметров и сценариев работы реле.

**А.1.10**
**последствия**
количественные показатели серьезности риска или опасного события

**А.1.11**
**контроль (технический контроль безопасности)**
средство для уменьшения рисков в системе информационной безопасности

**А.1.12**
**межсайтовый скриптинг**
тип уязвимости в системе информационной безопасности, который позволяет злоумышленникам внедрить скрипт со стороны браузера системы защиты и управления, которым пользуется клиент

ПРИМЕЧАНИЕ Взаимодействующие браузеры приложений систем защиты и управления ссылаются на неограниченные вводные данные пользователя. Злоумышленники внедряют вредоносный код посредством этих вводных данных, вызывая тем самым непреднамеренное выполнение скрипта в браузере клиента.

**А.1.13**
**информационная защита**
все необходимые технические и нетехнические меры для защиты информационных систем защиты и управления

**А.1.14**
**информационная безопасность**
желаемое условие работы системы защиты и управления, которое позволяет ей выдерживать события злонамеренного происхождения, ставящие под угрозу доступность, целостность или конфиденциальность хранящихся, обрабатываемых или передаваемых данных, или услуг, предоставляемых системой защиты и управления

**А.1.15**
**древо решений**
инструмент поддержки принятия решений, который использует древовидный граф или модель решений и их возможных последствий, включающих исходы случайных событий, стоимость ресурсов и функцию полезности

ПРИМЕЧАНИЕ Операционные исследования обычно используют древо решений, в частности в анализе решений, чтобы помочь определить стратегию, которая наиболее подходит для достижения цели.

**А.1.16**
**надежность**
исследование неисправностей и отказов системы защиты и управления для того, чтобы обеспечить ее способность выполнять свои функции, при определенных условиях в течение заданного периода времени

**А.1.17**
**дроппер**
программа или набор программ, скрывающих себя за счет неисправностей или отклонений механизмов безопасности компьютера, что позволяет удаленным пользователям тайно контролировать операционную систему компьютера

**А.1.18**
**крайняя точка**
один из двух компонентов, который реализует и предоставляет интерфейс для других компонентов или использует интерфейс другого компонента [ISO / МЭК 24791-2: 2011]

**А.1.19**
**отпечаток пальца**
короткий и компактный код, который может быть вычислен для того, чтобы охарактеризовать некоторую заданную информацию, и обладает таким свойством, что практически невозможно построить другую информацию, которая дала бы такой же вывод [ISO / МЭК 8613-1: 1994]

**А.1.20**
**межсетевой экран**
устройство, которое реализует политику разделения между несколькими сетями с помощью фильтрации потоков данных между ними

**А.1.21**
**прошивка**
сочетание аппаратных устройств и компьютерных инструкций или данных, которые находятся только в формате для чтения программного обеспечения на аппаратном устройстве [ISO / МЭК / IEEE 24765: 2010]

**А.1.22**
**частотные модели**
наборы позиций, подмножеств, подпозиций, которые появляются в наборе данных с определенным уровнем частоты [37]

**А.1.23**
**сервер архивных данных**
база данных, содержащая журналы аварийных сигналов и информацию о процессах, собранных с помощью программного обеспечения систем защиты и управления

ПРИМЕЧАНИЕ сервер архивных данных часто ограничен системой защиты и управления или централизован.

**А.1.24**
**человеко-машинный интерфейс (HMI)**
устройство или компонент устройства, позволяющий третьему лицу взаимодействовать и управлять работой системы защиты и управления

**А.1.25**
**инцидент (в системе информационной безопасности)**
незапланированное прерывание службы, снижение качества обслуживания или событие, которое еще не повлияло на услугу, предоставляемую клиенту [ISO / МЭК 20000-1: 2011]

**А.1.26**
**интеллектуальное электронное устройство (IED)**
устройства защиты и управления, основанные на микропроцессорах

**A.1.27**
**жизненный цикл**
эволюция системы, продукта, услуги, проекта или другого сделанного человеком объекта с момента начала работы до вывода из эксплуатации [ISO / МЭК 15288 и ISO / МЭК 12207]

**A.1.28**
**локальное (управление)**
(прил.) модифицированный диапазон терминов, который представляет собой единое пространство процесса [словарь института инженеров электротехники и электроники, седьмое издание]

ПРИМЕЧАНИЕ используйте локальное управление только из технологического пространства объекта (подстанции). Для этой технической брошюры, данный термин установлен в пределах объема данного исследования.

**A.1.29**
**атака через посредника**
активное перехватывание информации, при котором злоумышленник осуществляет независимые соединения с сетью связи систем защиты и управления [измененное определение из Википедии]

ПРИМЕЧАНИЕ Наличие подключения к сети связи систем защиты и управления в пределах подстанции или снаружи по отношению к подстанции неизвестно законному отправителю и приемнику, поэтому законные лица считают такую связь частной, когда на самом деле злоумышленник контролирует весь трафик сообщений.

**A.1.30**
**сжатая форма сообщений**
представление текста в виде одной строки цифр, созданной с использованием формулы, которая называется односторонней хэш-функцией

ПРИМЕЧАНИЕ шифрованная сжатая форма сообщения с помощью закрытого ключа создает цифровую подпись, которая является электронным средством аутентификации.

**A.1.31**
**система защиты и управления**
совокупность интеллектуальных электронных устройств и устройств локальной сети на подстанции

**A.1.32**
**корень доверия**
незаконный сертификат открытого ключа или самостоятельно подписанный сертификат, который выявляет корневой центр сертификации (CA).

ПРИМЕЧАНИЕ корневой центр сертификации является частью ключевой схемы общественной инфраструктуры. Наиболее широкий коммерческое диапазон соответствует стандарту ITU-T X.509, который обычно включает в себя цифровую подпись центра сертификации (CA).

**A.1.33**
**параметры**
численные описания, которые позволяют пользователям настраивать функции защиты и управления в соответствии с расчетными параметрами

ПРИМЕЧАНИЕ ДЛЯ ВВОДА обычно доступ к настройке программ IED используется для чтения / записи команд с целью изменения значений параметров

**A.1.34**
**дистанционное обслуживание**
диагностики программ IED выполняется за пределами системы защиты и управления

**A.1.35**
**очистка (фильтрация)**
практика кодирования или устранения опасных элементов в ненадежных данных [38]

процесс принятия или отклонения потоков данных через сеть, в соответствии с определенными критериями [ISO / МЭК 27033-1: 2009]

**А.1.36**
**уровень обеспечения безопасности**
мера защиты системы информационной безопасности, полученная в соответствии с конкретной шкалой с использованием метода обеспечения надежности [изменен на основе стандарта ISO / МЭК 19792: 2009]
ПРИМЕЧАНИЕ 1 Признанная спецификация для получения воспроизводимых результатов обеспечения

ПРИМЕЧАНИЕ 2 Степень обеспечения безопасностью не может быть измерена в абсолютных значениях, но может представлять собой относительную величину, которая приводится к эталонному значению

**А.1.37**
**критерий безопасности**
характеристика активов системы защиты и управления, позволяющая оценивать наличие различных уровней конфиденциальности

ПРИМЕР доступность, целостность, конфиденциальность, отслеживаемость событий

**А.1.38**
**инцидент в системе безопасности**
одно или более нежелательное или неожиданное событие, связанное с нарушенными операциями системы защиты и управления

**А.1.39**
**последовательный анализ образцов**
открытие часто встречающихся последовательностей [37]

**А.1.40**
**серверная сторона**
операции, выполняемые с помощью сервера системы защиты и управления или сетевого IT-сервера в отношениях клиент-сервер в области компьютерных сетей

ПРИМЕЧАНИЕ 1 Как правило, сервер представляет собой программное обеспечение, такое как приложение браузера системы защиты и управления, которое работает на удаленном компоненте системы защиты и управления, доступном из локального компьютера или рабочей станции пользователя или собственных устройств сотрудников.

ПРИМЕЧАНИЕ 2 Операции могут выполняться на стороне сервера, так как им необходим доступе к информации или функциональности, которая недоступна на клиентском компьютере, или требует типичного поведения, которое является ненадежным, если сделано на стороне клиента.

**А.1.41**
**настройка**
параметры, определяющие функциональную сторону системы защиты и контроля

ПРИМЕЧАНИЕ В интеллектуальных электронных устройствах настройка не изменяет алгоритмы в программном обеспечении.

**А.1.42**
**группа настроек**
конкретный набор значений, связанный с применением одной защиты

ПРИМЕЧАНИЕ ДЛЯ ВВОДА Одно реле защиты может иметь несколько групп настроек, но только одна группа настроек активируется в каждый момент времени.

**А.1.43**
**программа установки**
компьютерное приложение, которое позволяет получить доступ к внутренним параметрам

настройки в интеллектуальных электронных устройствах

ПРИМЕЧАНИЕ ДЛЯ ВВОДА Программы установки ключа могут работать в автономном режиме или в режиме онлайн при подключении интеллектуальных электронных устройств.

**А.1.44**
**дробление стека(в системе защиты и управления)**
намеренное использование переполнения стека с целью получения контроля над системой защиты и управления

**А.1.45**
**целостность системы (защиты и управления)**
способность системы нормальным образом, свободно от преднамеренного или случайного несанкционированного манипулирования, выполнять свои функции, [на основе ISO 27799: 2008]

**А.1.46**
**схемы защиты системы целостности (защиты и управления)**
набор специальных схем защиты (SPS), схем устранения неисправностей (RAS) и других схем[39]

ПРИМЕЧАНИЕ Другие схемы включают в себя понижение частоты (UF), напряжения (UV) и несинхронизациую (OOS), но не ограничены данными параметрами .

**А.1.47**
**угроза**
потенциальная причина нежелательной инцидента, который может нанести вред системе защиты и управления

**А.1.48**
**сценарий угрозы**
описывает методы произведения кибератак

ПРИМЕЧАНИЕ ДЛЯ ВВОДА Сценарий представляет собой соединение источников, которые могут быть причиной угроз, дополнительными средствами атаки, критериями безопасности и уязвимости, которые делают возможным появление угрозы.

**А.1.49**
**подготовка (по вопросам информационной безопасности)**
приобретение знаний, навыков и компетенций в результате обучения профессионально-техническим или практическим навыкам и знаниям, которые касаются конкретных полезных компетенций

ПРИМЕЧАНИЕ IT–подготовка (по вопросам информационной безопасности) необходима для сетевых устройств локальной сети. Инженеры систем защиты и управления, а также технический персонал нуждается в обучении вопросам информационно безопасности для знания компонентов системы защиты и управления, которые подключаются к локальной сети. Как для инженеров, так и для технического персонала данная подготовка должна быть внесена в список должностных обязанностей.

**А.1.50**
**уязвимость**
характеристики активов системы защиты и управления, представляющие собой слабые места или недостатки, относящиеся к безопасности информационной системы

ПРИМЕР доверчивость персонала, простота входа на сайт системы защиты и управления, легкость доступа к системе или сети защиты и управления, возможность создавать или изменять системные команды.

**А.1.51**
**Вайтлистинг**
список или реестр лиц, которым по той или иной причине предоставляется конкретная привилегия, обслуживание, мобильность, доступ или идентификация.

## A.2 Используемые сокращения

| | |
|---|---|
| AAA | аутентификация, авторизация и учёт |
| ACL | список контроля доступа |
| ANSI | Американский национальный институт стандартов |
| AIC | доступность, целостность и конфиденциальность |
| BYOD | концепция использования сотрудниками собственных устройств (включая персональные компьютеры, планшетные устройства, мобильные телефоны) |
| CA | центр сертификации |
| CDV | проект стандарта, рассматриваемый техническим комитетом |
| CERC | способность компьютерной системы реагировать на аварийную операцию |
| CERT | экспертная группа по вопросам компьютерной безопасности в сети |
| CIGRE | Международный совет по большим электрическим системам высокого напряжения |
| CIM | общая информационная модель |
| CKM | конструктивное управление ключами защиты |
| CNN | информационный канал кабельного телевидения |
| CVE | распространённые уязвимости и риски |
| CySeMoL | язык моделирования информационной безопасности |
| DES | стандарт шифрования данных |
| DLL | динамически подключаемая библиотека |
| DNP | протокол распределенной (вычислительной) сети |
| DoS | отказ в обслуживании |
| DOS | дисковая операционная система |
| DSAS | цифровая система автоматизации подстанции |
| DFR | цифровой регистратор аварий |
| EAP | расширенный протокол аутентификации |
| EPU | электроэнергетическая компания |
| ESP | периметр электронной защиты |
| FAT | приемо-сдаточные испытания изготовителя |
| FBCA | центр сертификации «Federal Bridge» |
| FDIS | окончательный проект международного стандарта |
| FTP | протокол передачи файлов |
| GDOI | группа доменов интерпретации |
| GMC | эталонные часы |
| GOOSE | общие объектно-ориентированные события на подстанции |
| HBFW | межсетевой экран узлов |
| HMAC | хеш-код аутентификации сообщений |
| HMI | человеко-машинный интерфейс |
| IACS | автоматизация производства и системы управления |
| ICCP | протокол обмена данными между центрами управления |

| | |
|---|---|
| АСУ | автоматизированная система управления |
| IDS/IPS | система обнаружения вторжений / предотвращения вторжений |
| МЭК | международная электротехническая комиссия |
| IED | интеллектуальное электронное устройство |
| IEEE | институт инженеров электротехники и электроники |
| IP | межсетевой протокол |
| IRS | информационно-поисковая система |
| ISA | международное общество автоматизации |
| ISO | международная организация стандартизации |
| IT | информационные технологии |
| JWG | объединенная рабочая группа |
| KDC | центр распределения ключей |
| LAN | локальная сеть |
| LDAP | облегченный протокол доступа к сетевому каталогу |
| MAC | код идентификации сообщения |
| MPLS | многопротокольная коммутация меток |
| Мвар | реактивная мощность, мегавар |
| МВт | активная мощность, мегаватт |
| MMS | служба производственных сообщений |
| NERC | Североамериканская корпорация по обеспечению надёжности электроэнергетических систем |
| NIST | Национальный институт стандартов и технологий |
| NOP | пустая операция |
| OOS | несинхронизированный |
| ОС | операционная система |
| P&C | защита и управление |
| ПК | персональный компьютер |
| PCAST | совет по развитию науки и техники при президенте США |
| PЗI | предусмотренная возможность совершенствования изделия |
| PHP | язык создания персональных веб-страниц (препроцессор гипертекста, рекурсивный акроним) |
| PKI | инфраструктура с открытыми ключами |
| PLC | программируемый логический контроллер |
| PMU | устройство измерений векторных параметров |
| PSP | периметр физической защиты |
| PSRC | комитет по релейной защите в энергетических системах |
| PV | зависимость мощности от напряжения (кривые зависимости мощности от напряжения) |
| QoS | качество обслуживания |
| RA | адрес возврата |
| RAS | схема устранения неисправностей |
| RBAC | ролевое управление доступом |
| RDP | протокол удаленного рабочего стола |
| RFC | запрос комментария |

| | |
|---|---|
| ПЗУ | постоянное запоминающее устройство |
| RP&C | действующая защита и управление |
| RTS | корень доверия для хранения |
| RTU | блок дистанционного управления |
| SAG | консультативная группа правообладателей |
| SAT | приемочные испытания на месте эксплуатации |
| SC | исследовательский комитет |
| SCADA | диспетчерское управление и сбор данных |
| SHA | защищенный алгоритм хеширования |
| ПА | противоаварийная автоматика |
| SMIB | база информации управления безопасностью |
| SME | эксперт в предметной области |
| SNMP | упрощенный протокол управления сетью |
| SPDU | протокольный блок данных сеансового уровня |
| SPS | специальная система защиты |
| SQL | язык структурированных запросов |
| SSH | безопасная оболочка |
| SSL | протокол безопасных соединений |
| SV | выборочное значение |
| TACACS+ | система управления доступом для контроллера доступа к терминалу «плюс» |
| TASE | дистанционное управление прикладным сервисным элементом |
| TB | специальная брошюра |
| TCB | комплекс средств безопасности вычислительной системы |
| TLS | локальная память потоков |
| ToR | техническое задание |
| TR | технический отчёт |
| TSO | сетевая компания |
| UDP | протокол дейтаграмм пользователя |
| UF | пониженная частота |
| USB | универсальная последовательная шина |
| UV | пониженное напряжение |
| VNC | система управления удаленным компьютером |
| VPN | виртуальная частная сеть |
| VRF | виртуальная маршрутизация и переадресация |
| WAMPAC | система мониторинга защиты и управления |
| WAMS | система мониторинга переходных процессов |
| WAN | распределенная сеть |
| WEP | протокол обеспечения конфиденциальности |
| WLAN | беспроводная локальная сеть |
| WIB | Международная ассоциация «Instrumentation Users» |
| Wi-Fi | беспроводная передача данных |

| | |
|---|---|
| WSUS | сервис обновлений сервера Windows |
| XML | расширяемый язык разметки |
| XSS | межсайтовый скриптинг |
| YE | конец года |

# Приложение B

## Список литературы


[1] E. R. Egozcue, Dannie Herreras, J. A. V. Ortiz, Victor Fidalgo, and L. Tarrafeta, "Smart Grid Security - Recommendations for Europe and Member States," European Network and Information Security Agency 2012-07-01.

[2] F. Cleveland, "IEC TC57 security standards for the power system's information infrastructure - Beyond simple encryption," Report October 2006.

[3] TC65WG10, "Industrial communication networks - Network and system security - Part 2-4: Installation and maintenance service providers," International Electrotechnical Commission Geneva CH, Standard (Committee Draft for Vote), 62443/CDV-2-4, 2013-11-08.

[4] M. Morisse, B. Horlach, W. Kappenberg, J. Petrikina, F. Robel, and F. Steffens, "Trust in Network Organizations - A Literature Review on Emergent and Evolving Behavior in Network Organizations," in *47th Hawaii Internation Conference on System Sciences*, Waikoloa, Hawaii, 2014, pp. 4578-4587.

[5] "Report to the President - Immediate opportunities for strengthening the nation's cybersecurity," The President's Council of Advisors on Science and Technology 2013.

[6] K. Tsipenyuk, B. Chess, and G. McGraw, "Seven pernicious kingdoms: A taxonomy of software security errors," *Security & Privacy, IEEE,* vol. 3, pp. 81-84, 2005.

[7] D. Mitropoulos, V. Karakoidas, P. Louridas, and D. Spinellis, "Countering code injection attacks: a unified approach," *Information Management & Computer Security,* vol. 19, pp. 177-194, 2011.

[8] One, "Smashing the stack for fun and profit," *Phrack magazine,* vol. 7, pp. 14-16, 1996.

[9] T. Sommestad, H. Holm, and M. Ekstedt, "Effort estimates for vulnerability discovery projects," in *45th Hawaii International Conference on System Sciences*, Maui, 2012, pp. 5564-5573.

[10] T. Sommestad, H. Holm, and M. Afzal, "Security mistakes in information system deployment projects," *Information Management and Computer Security,* vol. 19, 2011.

[11] T. Sommestad, M. Ekstedt, H. Holm, and M. Afzal, "Security mistakes in information system deployment projects," *Information Management & Computer Security,* vol. 19, pp. 80-94, 2011.

[12] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Periner, W. T. Polk, S. Gupta*, et al.*, "Electronic Authentication Guideline," Gaithersburg MD, Special Publication 800-63-1, December 2011.

[13] J. Cazier, "Password security: An emperical investigation into e-commerce passwords and their crack times," *Information Security Journal: A Global,* 2006.

[14] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, Indiana: Wiley, 2002.

[15] S. Abraham and I. Chengalur-Smith. (2010, August) An overview of social engineering malware: trends, tactics and implications. *Technology in Society*. 183-196.

[16] H. Huang, J. Tan, and L. Liu, "Countermeasure Techniques for Deceptive Phishing Attack," in *2009 International Conference on New Trends and Service Science*, June 2009, pp. 636-641.

[17] M. Jakobsson. (2009) Modeling and preventing phishing attacks. *Lecture notes in computer science*. 89.

[18] P. Syverson. (1994) A taxonomy of replay attacks. *IEEE Computer Society Press*.

[19] D. Dxung, M. Naedele, T. P. Von Hoff, and M. Crevatin, "Security for Industrial Communication Ssytems," in *Proceedings of the IEEE*, 2005, pp. 1152-1177.

[20] (2010, Man in the Middle Attack. *CAPEC - Common Attack Pattern Enumeration and Classification*. Available: http://capec.mitre.org/data/difinitions/94.html

[21] TC57WG15, "Power systems management and associated information exchange: Data and Communication Security - Security for IEC 61850," International Electrotechnical Commission, Standard IEC 62351-6, January 2007 (NOTE a new version will be released).

[22] "Communication networks and systems for power utility automation - Part 90-5: use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118," Technical Report IEC/TR 61850-90.5 ed 1.0, 2012-05-09.

[23] "Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3,"

International Electrotechnical Commission, Standard IEC 61850-9-2 Ed. 2.0, 2011.
[24] "Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3," Standard IEC 61850-8-1 Ed. 2, 2011.
[25] M. Baugher, B. Weis, T. Hardjono, and H. Harney, "The Group Domain of Interpretation," The Internet Society, Request for Comment (RFC) RFC 3547, July 2003.
[26] TC57WG15, "Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment," International Electrotechnical Commission, Standard IEC/CDV 62351-9, March 2013.
[27] R. Langner, "To Kill a Centrifuge," http://www.langner.com/en/wpcontent/uploads/2013/11/To-kill-a-centrifuge.pdf 2013.
[28] A. Dufkova, J. Budd, J. Homola, and M. Marden, "Good practice guide for CERTs in the area of Industrial Control Systems," Technical Report, October 2013.
[29] WG-B5.31, "Life-time management of relay settings," CIGRE, Technical Brochure, 2012.
[30] "Life-time management of relay settings," Final Draft2012.
[31] "The Vensim Simulation Environment," vol. Vensim PLE for Windows 6.2a-1 ed: Ventanna Systems, Inc - Vensim Product Center.
[32] J. D. Sterman, *Business Dynamics - System thinking and modeling for a complex world*: McGraw-Hill Higher Education 2000.
[33] J. Hernantes, A. Lauge, L. Labaka, E. Rich, F. O. Sveen, J. M. Sarriegi*, et al.*, "Collaborative modeling of awareness in Critical Infrastructure Protection," presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference on, 2011.
[34] J. Hernantes, A. Lauge, L. Labaka, E. Rich, F. O. Sveen, J. M. Sarriegi*, et al.*, "Coolaborative modeling of awareness in critical infrastructure protection," in *Proceedings of the 44th Hawaii International Conference on System Sciences*, 2011, pp. 1530-1605.
[35] J. Wiik, J. J. Gonzalez, H. F. Lipson, and T. J. Shimeall, "Dynamics of vulnerability - modeling the life cycle of software vulnerabilities," Technical Report2004.
[36] T. Sommestad, M. Ekstedt, and H. Holm, "The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise Sysem Architectures," *IEEE Systems Journal*.
[37] C. B. Simmons, S. Shiva, V. Phan, V. Shandilya, and L. Simmons, "IRS: An Issue Resolution System for Cyber-Attack Classification and Management," in *The 2012 International Conference on Security & Management*, Las Vegas, NV USA, 2012, pp. 53-59.
[38] J. Weinberger, P. Saxena, D. Akhawe, M. Finifter, R. Shin, and D. Song, "A systematic analyssis of XSS sanitization in web application frameworks," in *ESORICS 2011*, Berlin Heidelberg, 2011, pp. 150-171.
[39] V. Madani, M. Begovic, D. Novosel, and M. Adamiak. (2010, October) Application considerations in system integrity protection schemes (SIPS). *Power Delivery, IEEE Transactions on*. 2143 - 2155.
[40] C. W. B5.38, "The impact of implementing cybersecurity requirements using IEC61850," Technical Brochure CIGRE TB #427, August 2010.
[41] C. W. B5.22, "Wi-fi protected access for protection and automation," Technical Brochure CIGRE TB #318, April 2007.
[42] "Security profile for substation automation," Security Profile Draft 0.15, September 12, 2012.
[43] "Requirements for Secure Control and Telecommunication Systems," White Paper2008-10-06.
[44] I. TC57WG15, "Power system management and associated information exchange: Data and Communication Security - Security for IEC 61850," Standard IEC 62351-6, January 2007.
[45] I. TC57WG15, "Power systems management and associated information exchange: Data and communication security - Profiles including MMS," Standard IEC 62351-4, January 2007.
[46] I. TC57WG15, "Power systems management and associated information exchange: Data and communication security - Profiles including TCP/IP," Technical Specification IEC 62351-3, January 2007.
[47] I. TC57WG15, "Power systems management and associated information exchange: Data and communication security - Role-based access control," Draft IEC 62351-8, To be published.

[48] "Security for industrial process measurement and control - Network and system security, Part 1-1: Concepts, models and terminology," Technical Specification IEC/TS 62443-1-1, 2005.
[49] "Security for industrial process measurement and control - Network and system security, Part 2-1: Establishing an industrial automation and control system security program," Standard IEC/0CD 62443-2-1.
[50] "Security for industrial process measurement and control - Network and system security, Part 3-3:," Draft Standard IEC/CDV 62443-3-3, 2011.
[51] *Security for industrial process measurement and control - Network and system security Part 2-4:: Requirements for Security Programs for IACS Integration and Maintenance Service Providers*. Geneva, Switzerland: IEC, 2013-11-08.
[52] "Process Control Domain - Security Requirements for Vendors," International Instrument Users Associations - EWE, The Netherlands, Requirements Specification M2784-X-10, Second Issue, Index Classification 50.1, Version 2.0, October 2010.
[53] "Standardization Mandate for Smart Grid," Guideline - Mandate M/490, 2012.
[54] "Protection and Control Systems Cybersecurity Practices," ReportOctober 2012.
[55] L. K. Shar and H. B. Kuan Tan. (2012, March) Defending against cross-site scripting attacks. *Computer*. 55-62.
[56] J. Walker, M. E. Kounavis, S. Gueron, and G. Graunke. (2012, July) The theory, design, and implementation of cryptogrphic hash functions. *Dr Dobbs Journal*. 17-30.
[57] O. Mueller. (2012, July) Preventing Stack Overflow Attacks. *Dr Dobbs Journal*. 7-16.
[58] F. T. Sheldon and C. Vishik. (2010, September) Moving toward trustworthy systems: R&D essentials. *Computer Software Assurance*. 31-40.
[59] T. Sommestad, M. Ekstedt, and H. Holm, "The Cyber Secuirty Modeling Language: a tool for assessing the vulnerability of enterprise system architectures," *IEEE Systems Journal,* vol. PP, December 11 2012.
[60] R. Cooke, *Experts in Uncertainty - opinions and subjective probability in sience*. New York, New York USA: Open University Press, 1991.
[61] M. Buschle, H. Holm, T. Sommestad, M. Ekstedt, and K. Shahzad, "A tool for automatic enterprise architecture modeling," in *CAiSE Forum*, 2011, pp. 25-32.
[62] E. S. Chew, Marianne; Stine, Kevin; Bartol, Nadya, Brown, Anthony; Robinson, Will "Perfomance Measurement Guide for Information Security," I. T. L. Computer Security Division, Ed., ed: National Institute of Standards and Technoloby, July 2008.
[63] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for Key Management - Part 1: General (Revised)," I. T. L. Computer Security Division, Ed., ed: National Institute of Standards and Technology, March 2007.
[64] ANSI, "Framework for Key Management Extensions," ANSI X9.69.
[65] V. Madani, D. Novosel, S. Horowitz, M. Adamiak, J. Amantegui, D. Karlsson*, et al.*, "IEEE PSRC report on global industry experiences with system integrity protection schemes (SIPS)," *IEEE Transactions on Power Delivery,* vol. 25, pp. 2143-2155, 2010.
[66] "Global Industry Experiences with System Integrity Protection Schemes (SIPS)," IEEE PSRC2009.
[67] "Security for industrial automation and control systems: Patch Management in an IACS Environment," Technical Report IEC/DTR 62443-2-3.
[68] E. Ogren, "Enpoint Security: Moving Beyon AV," An Ogren Group Special ReportJuly 2009.
[69] "The impact of implementing cybersecurity requirements using IEC 61850," Technical Brochure 427, August 2010.

# Приложение С

## Примеры электрических систем под воздействием кибератак

Рассмотрим систему, показанную на рисунке С-4. На нем представлена система напряжением 735 кВ, состоящая из 3 линий по 800 км, которая питает нагрузку мощностью 3000 МВт. Эта система является отрегулированной, уровни напряжений равны номинальным, что достигается использованием шунтирующих реакторов мощностью 2310 Мвар на первой подстанции и мощностью 1320 Мвар на второй подстанции. Допустим, что в данной электроэнергетической компании отсутствует противоаварийная автоматика (ПА), и диспетчер выполняет маневр с пульта управления. Предположим, что существует взломщик, который способен получить доступ к такому IED, как, например, реле дифференциальной защиты линии. Взломщик решил запустить команду на отключение выключателя одной из трех линий электропередач.

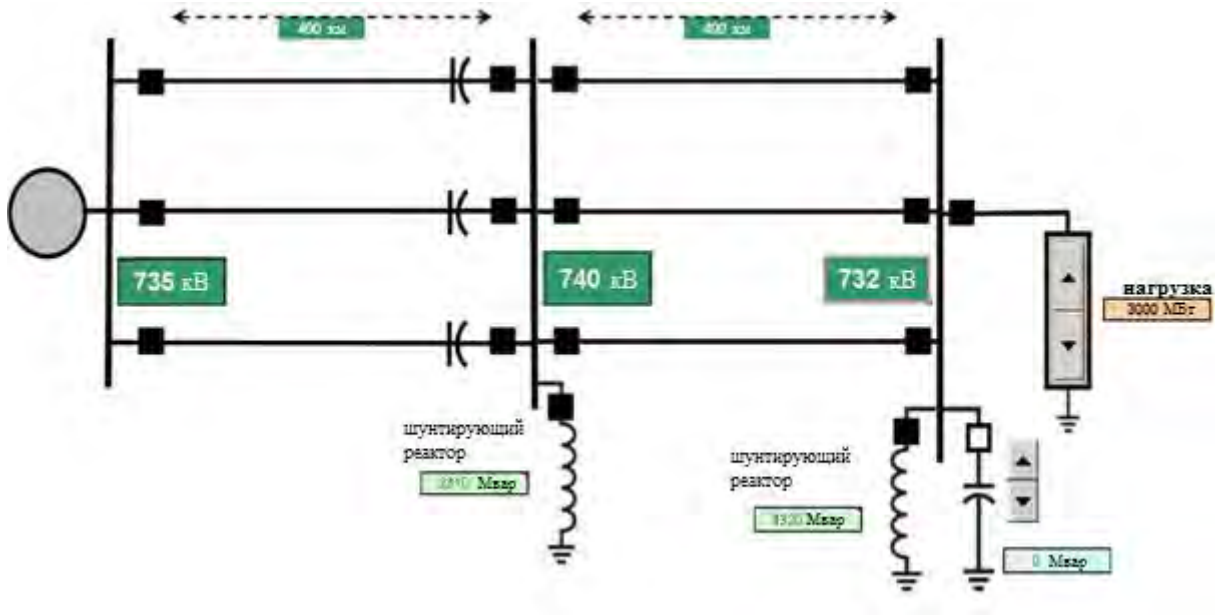



**Рисунок С-4 Пример системы напряжением 735 кВ**

На рисунке С-5 можно увидеть, что напряжение упало до 618 кВ на первой подстанции и до 564 кВ на второй подстанции. В данной ситуации система становится неустойчивой, и действия диспетчера направлены на возвращение уровней напряжения к номинальному уровню.

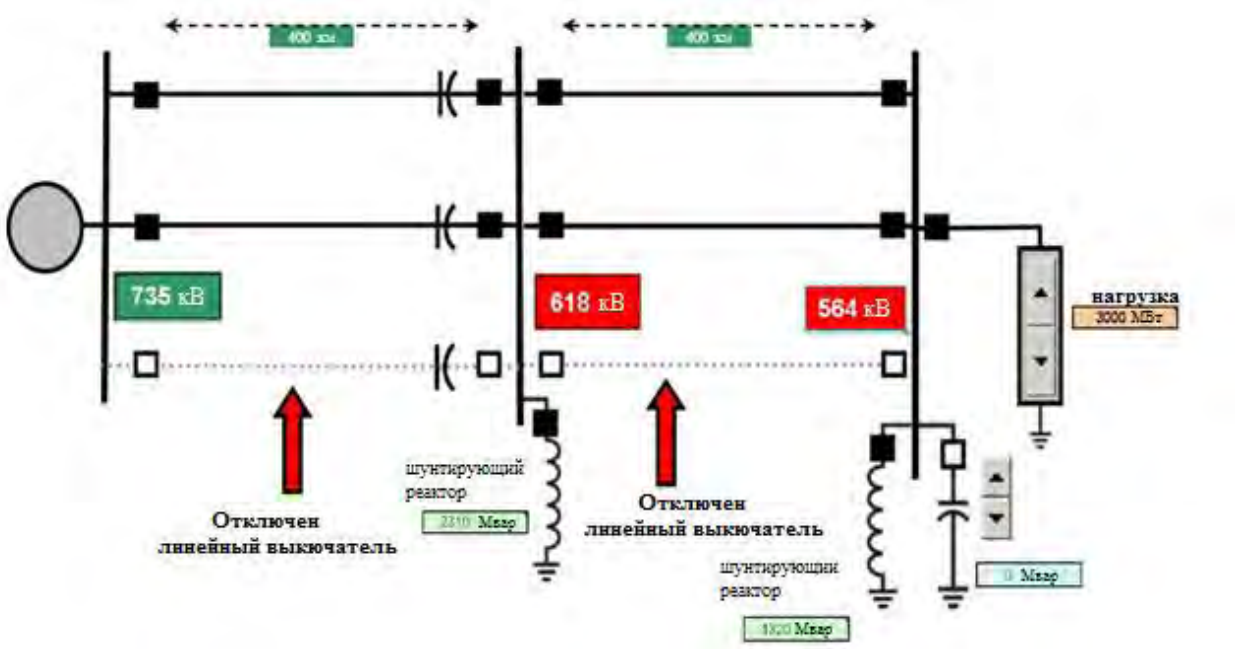



**Рисунок С-5 Влияние отключения, вызванного кибератакой**

Диспетчеру необходимо уменьшить определенное количество реактивной мощности шунтирующих реакторов на двух подстанциях для того, чтобы отрегулировать систему (рисунок С-6). Благодаря уменьшению мощности шунтирующего реактора на 1320 МВАр на первой подстанции и на 825 МВАр на второй подстанции система становится устойчивой, и уровень напряжения снова возвращается к номинальному уровню.

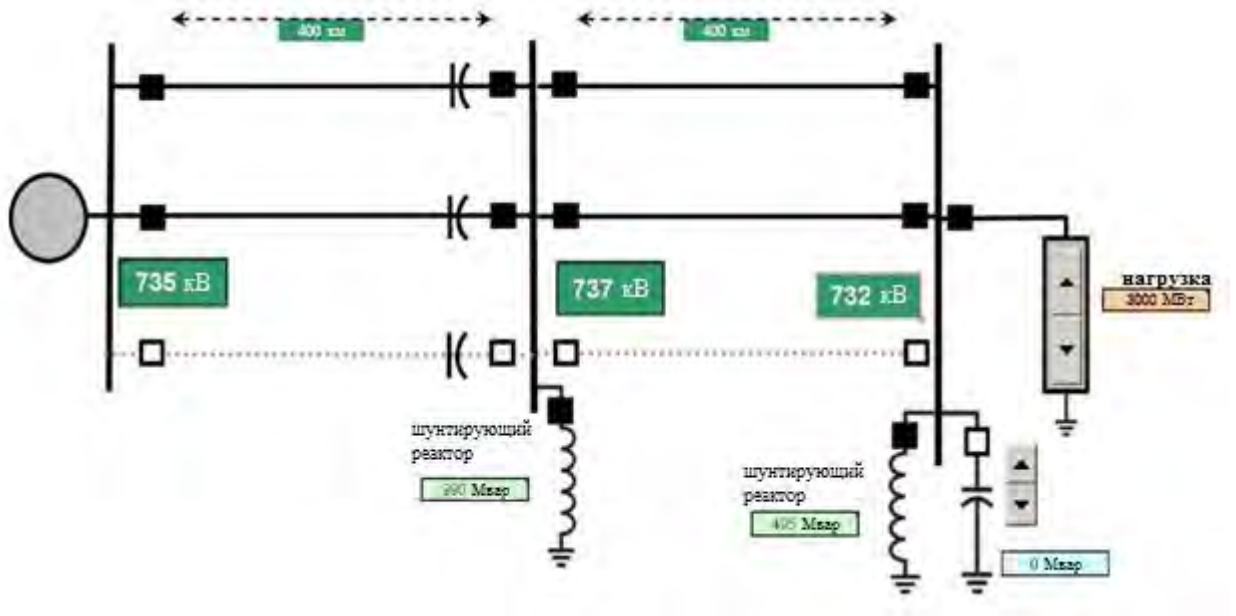



**Рисунок С-6 Регулирование сети путем уменьшения реактивной мощности**

Однако, теперь система становится слабой, так как в ней остаются две линии вместо трех. Таким образом, система является более чувствительной к возмущениям, показанным на рисунке С-7.

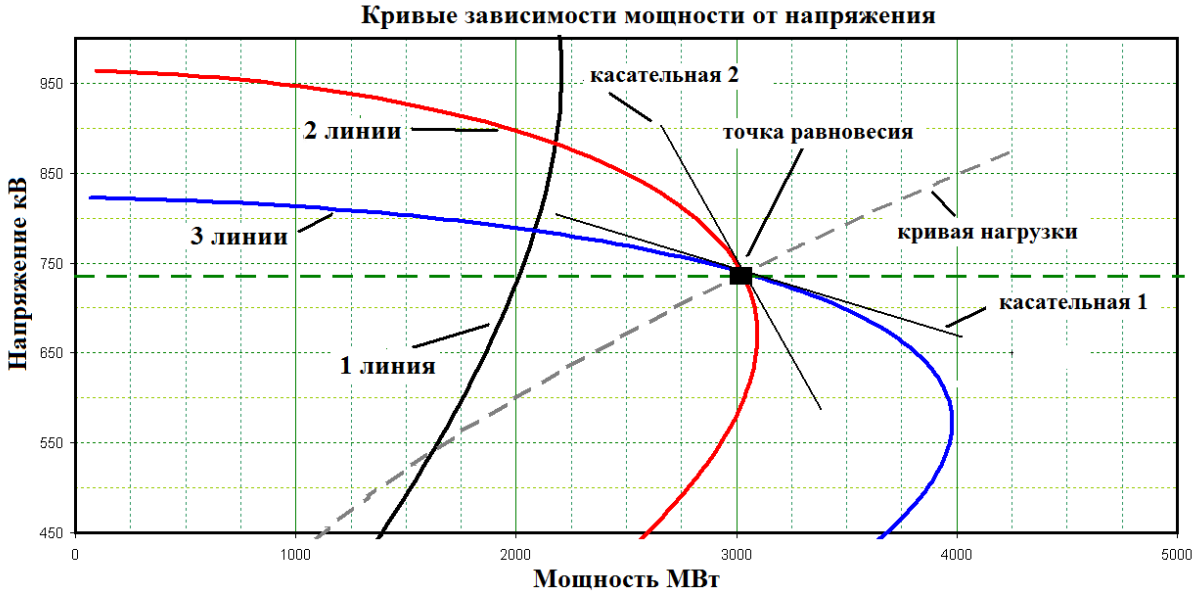



**Рисунок С-7 Результаты ослабленной системы**

Крутизна кривой зависимости мощности от напряжения для двух линий (касательная 2) имеет больший наклон, чем крутизна кривой для трех линий (касательная 1). Это означает, что при изменении передаваемой активной мощности (МВт), отклонение уровня напряжения от нормы теперь будет более серьезным, чем в случае системы с тремя линиями. Таким образом, сейчас система более чувствительна к возмущениям, и становится сложнее сохранить ее устойчивость. Отметим, что кривая зависимости мощности от напряжения для одной линии на рисунке С-7 показывает, что одной линии недостаточно, чтобы питать нагрузку 3000 МВт. Таким образом, в данном примере очевидно, что взломщик, который способен отключить две или более линий создаст перерыв в электроснабжении большого количества потребителей.

Рассмотрим другой пример, пусть существует отрегулированная система, похожая на ту, что показана на рисунке С-4. Однако в этот раз взломщик получил контроль над защитными реле шунтирующего реактора. Шунтирующие реакторы на подстанциях контролируют уровень напряжения системы. Влияние на систему в случае, если взломщик запустит команду на отключение выключателей шунтирующего реактора и исключит всю компенсацию реактивной мощности на подстанциях, было бы таким, как показано на рисунках С-8 и С-9.

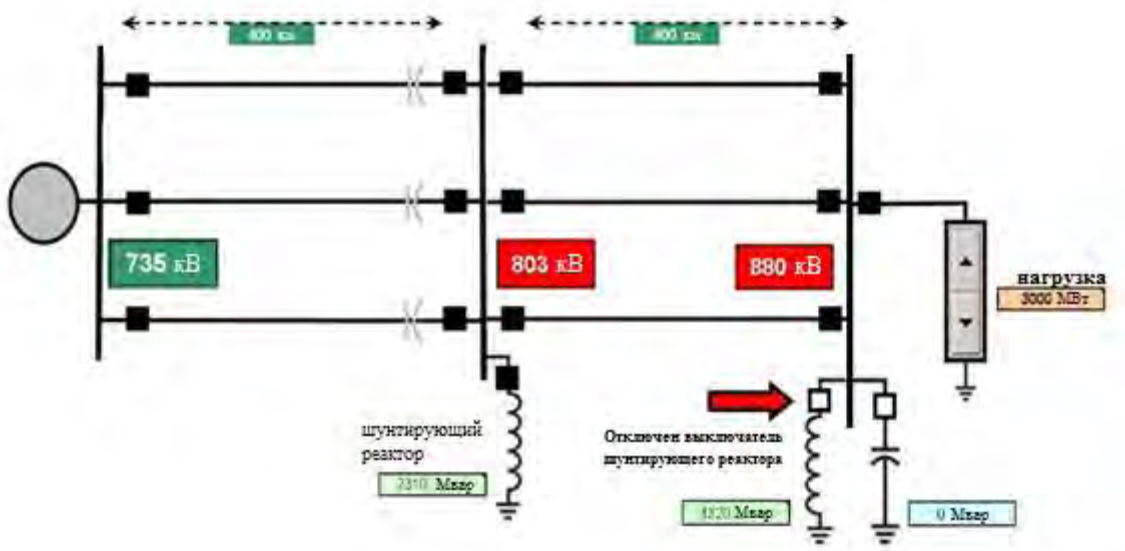



**Рисунок С-8 Влияние на систему в случае потери всей компенсации**

Рассмотрим график на рисунке С-9, черная кривая зависимости мощности от напряжения изображает систему с тремя линиями и поперечной компенсацией 1320 Мвар. Точка равновесия, расположенная на графике, соответственно изображает систему, отрегулированную в пределах 735 кВ с нагрузкой 3000 МВт (рисунок С-4). Предположим, что взломщик может контролировать защитные реле шунтирующих реакторов и запускает команду на отключение выключателей шунтирующего реактора. Система переходит в режим недокомпенсации реактивной мощности. На рисунке С-8 уровень напряжения на нагрузке повышается до 880 кВ (1,2 о.е.). Резкое увеличение напряжения может повредить электрооборудование или активировать другие защиты, которые могут вызвать реакцию серии отключений.

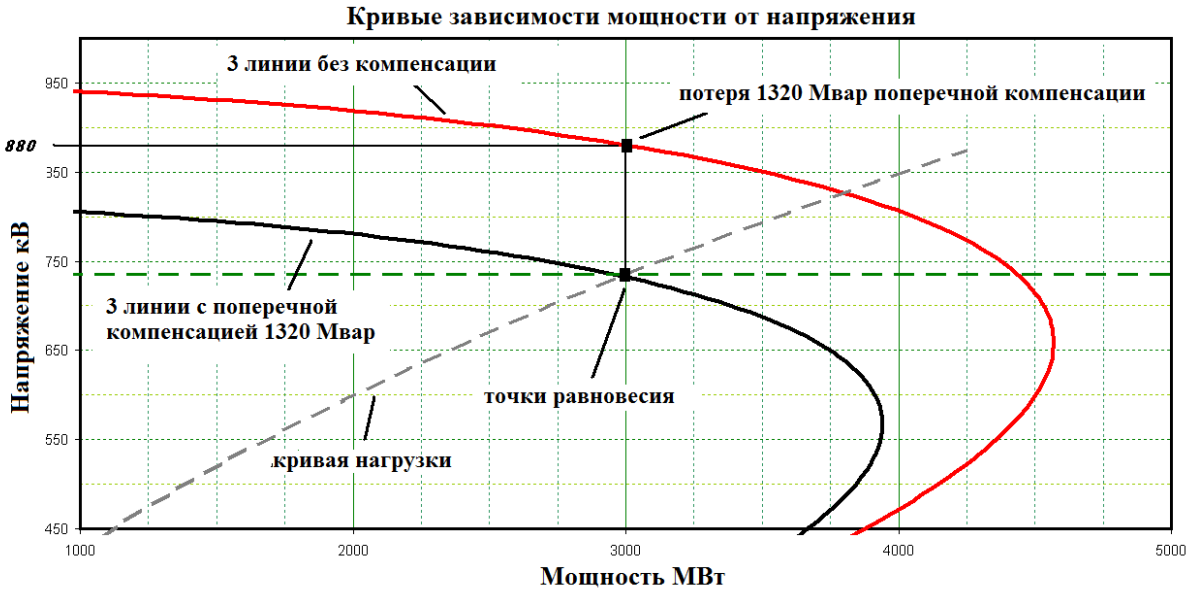



**Рисунок С-9 Потеря поперечной компенсации**

На графике (Рисунок С-9), точка равновесия сместилась до красной кривой зависимости мощности от напряжения, которая соответствует режиму без компенсации реактивной мощности. Уровень напряжения в системе повысился с 735 кВ до 880 кВ. К счастью, взломщик не отключил шунтирующий реактор первой подстанции, тогда результат был бы хуже.

# Приложение D
# Обзор действующих отчетов, стандартов и передовых практических методов

## D.1 Технический подход, который использовался для обзора публикаций в отрытом доступе и проведения оценок

### D.1.1 Введение

Более ранние работы CIGRE SC B5, изложенные в специальной брошюре №427[40] были использованы в качестве исходного пункта для этой работы. Включая обновления, выводы по предыдущей работе отражают текущее состояние рекомендаций по информационной безопасности, стандартов и наработанных методик.

### D.1.2 Отчеты по вопросам информационной безопасности систем защиты и управления

**Таблица D-6 Отчеты по вопросам информационной безопасности систем защиты и управления**

| Идентификатор отчета | Название отчета | Вопросы и трудности |
|---|---|---|
| CIGRE TB #427[40] | Последствия реализации требований информационной безопасности при использовании IEC 61850 | • Отсутствие безопасности в средствах конфигурирования<br>• Ни один стандарт или руководящее указание не эффективно обращается к управлению исправлениями системы защиты и управления.<br>• Отсутствие системы показателей информационной безопасности для оценки и количественного анализа уровня обеспечения безопасности. |
| CIGRE TB #318[41] | Защищенный доступ Wi-Fi для защиты и автоматизации | • Отсутствие руководящих указаний по применению IEEE 802.11i для систем защиты и управления. |
| ASP-SG[42] | Профиль защиты для автоматизации подстанций | • Ранний проект, но имеет потенциал к улучшению безопасности при реализации для инженеров защиты и управления. |
| Рабочая группа BDEW [43] | Технический документ: Требования к обеспечению контроля безопасности и к системам телекоммуникации | • Документ содержателен, но является более ИТ направленным, а не эксплуатационным для области защиты и управления. |

### D.1.3 Стандарты для защиты информационной безопасности систем защиты и управления

**Таблица D-7 Стандарты для защиты информационной безопасности систем защиты и управления**

| Идентификатор стандарта | Название стандарта | Оценка применимости |
|---|---|---|
| IEC 62351[44-47] | Управление энергетической | Требования к информационной безопасности для |

| Идентификатор стандарта | Название стандарта | Оценка применимости |
|---|---|---|
| | системой и связанный с ней обмен данными: информация и защита коммуникации | контроля использования и своевременной отчетности о событиях в системах защиты и управления малоэффективны.<br>Не рассматриваются характеристики информационной безопасности для ограничения потока данных и доступности сетевых ресурсов. Ролевое управление доступом (часть 8). |
| IEC 62443[48-50] | Безопасность при измерении и управлении в производственных процессах – безопасность сети и системы | Требования к информационной безопасности для контроля использования, целостности данных, конфиденциальности данных и ограничения потока данных в системах защиты и управления малоэффективны.<br>Не рассматриваются характеристики информационной безопасности для своевременной отчетности о событиях и доступности сетевых ресурсов. |
| IEEE 1686 | Стандарт IEEE о возможностях информационной безопасности интеллектуальных электронных устройств (IEDs) на подстанции | Дано детальное описание управления электронным доступом, журнала регистрации событий и т.д. для интеллектуальных электронных устройств (IED) на подстанции.<br>Не рассматривается связь с подстанцией по защищенным сетям, как по внутренним, так и внешним каналам связи. |
| IEEE 1711 | Экспериментальный стандарт криптографического протокола для информационной безопасности для линий последовательной передачи данных | В случае необходимости производят защиту конфиденциальности линий последовательной передачи данных, использованных для сигнализации в системах защиты и управления, или настройках интеллектуальных электронных устройств (IED).<br>Количество каналов последовательной передачи данных, используемых в настоящее время, уменьшается. |

Одной из областей, которую необходимо улучшить, является своевременная отчетность. Для того, чтобы быть полезной для инженеров защиты и управления, и для обеспечения логически связанных обзоров для контроля процессом управления необходимо нормализовать получаемые данные. После тщательной нормализации, корреляция событий, данных и контекстуальных данных из различных источников происходит их преобразование в логически связанную информацию. Для определенных целей автоматизированный анализ логически связанной информации облегчает мониторинг безопасности системы защиты и управления, мониторинг активности пользователей системы защиты и управления, а также отчетность о соответствии.

### D.1.4 Рекомендации по информационной безопасности систем защиты и управления

Перечисленные отчеты в таблице D-8 являются перечнями рекомендаций, включающими обязательные требования.

**Таблица D-8 Рекомендации по информационной безопасности систем защиты и управления**

| Идентификатор рекомендации | Название рекомендации | Оценка применимости |
|---|---|---|
| Отчет WIB[19] [51] | Домен управления технологическим процессом – требования к безопасности для разработчика | WIB 2.0 является опубликованным отчетом ( не относится к рекомендованным из-за нехватки важных требований, которым уделяют внимание в отчете WIB 3.0)<br><br>Рекомендация: использовать проект отчета для WIB 3.0 (последнее обновление проекта доступно на holsteindk@ieee.org)<br><br>Первый вариант отчета WIB 3.0 является исходной точкой для развития IEC 62443-2-4 (не рекомендуется до тех пор, пока не пройдет этап рассмотрения техническим комитетом(CDV) и не будет издан в виде окончательного проекта международного стандарта (FDIS) |
| M/490[52] | Требования к стандартизации «Умных сетей» (Smart Grid) | Включает описание Европейской Комиссией архитектурной модели «Умных сетей», уровни безопасности на основе анализа последствий, а также классы защиты для классификации и маркировки информационных моделей.<br><br>Рекомендация: согласовать анализ последствий в системах защиты и управления с уровнями безопасности M/490. |

## D.2 Результаты опроса о защите и управлении

### D.2.1 Порядок проведения опроса

В середине 2012 года компания Newton-Evans Research по поручению CIGRE JWG B5-D2.46 исследовала политику информационной безопасности в системах защиты и контроля в электроэнергетических компаниях.

Результаты этого отчета были основаны на ответах 63 электроэнергетических компаний со всего мира на протяжении июня, июля и августа 2012 года. На рисунке D-10 показано распределение голосов. Из 63 компаний, 25 были расположены в США и Канаде, в то время как 38 располагались в других странах. Компании США состояли из частных энергокомпаний (8), коммунальных предприятий (7) и кооперативных энергокомпании (4). Представители компаний были готовы к сотрудничеству и имели разумное понимание темы исследования и задаваемых вопросов.

[19] Международная ассоциация «Instrument Users» (WIB) обеспечивает процесс оценки измерительных приборов и услуг для ее пользователей - промышленных компаний. WIB работает в тесном сотрудничестве в федерации «SWE» с ассоциациями партнерами EXERA во Франции и SIREP/EI в Великобритании. Соглашение о сотрудничестве существует и с организацией NAMUR в Германии.


**Рисунок D-10 Распределение голосов опрашиваемых компаний**

### D.2.2 Вопросы, задаваемые в ходе исследования

Таблица D-9 содержит вопросы, которые задавались в ходе опроса организаций, занимающихся эксплуатацией систем защиты и управления ЭЭС, а также ИТ-организаций, ответственных за информационную безопасность систем защиты и управления и элементов сетей связи. В первой колонке указан номер вопроса. В следующих двух колонках содержатся вопросы и возможные варианты ответов. В последней колонке указана цель, преследуемая объединённой рабочей группой, или цель вопроса. В анкете, которую рассылали при исследовании, цели не указывались.

**Таблица D-9 Вопросы для исследования информационной безопасности систем защиты и управления**

| Номер вопроса | Вопрос | Варианты ответа | Цель вопроса |
|---|---|---|---|
| 1 | Проводите ли Вы обучение сотрудников (инженеров и технического персонала) служб защиты и управления по вопросам информационной безопасности? (В особенности, обучение, связанное с функциональными элементами систем защиты и управления, такими как подстанционные устройства защиты и управления и подстанционное оборудование локальных сетей, за исключением функциональных элементов системы SCADA). | ДА, НЕТ, ПЛАНИРУЕТСЯ к концу 2015 года | Оценка степени организации системы защиты и управления |
| 2 | Проводите ли Вы обучение по вопросам информационной безопасности в контексте должностных обязанностей персонала? | ДА, НЕТ, ПЛАНИРУЕТСЯ к концу 2015 года | Оценка эффективности программы обучения по вопросам информационной безопасности систем |

| Номер вопроса | Вопрос | Варианты ответа | Цель вопроса |
|---|---|---|---|
| 3 | Как Вы оцениваете качество и полноту программы обучения по вопросам информационной безопасности в Вашей организации? | ОЧЕНЬ ХОРОШО, ХОРОШО, СРЕДНЕ, ПЛОХО, ОЧЕНЬ ПЛОХО, НЕ ЗНАЮ | защиты и управления |
| 4 | Отразилось ли ухудшение экономической ситуации на мероприятиях по информационной безопасности систем защиты и управления в Вашей организации? | ДА, НЕТ | |
| 5 | Имеются ли в Вашей системе защиты и управления правила допустимого использования сети, подписанные сотрудниками? | ДА, НЕТ, ПЛАНИРУЕТСЯ к концу 2015 года, НЕ ЗНАЮ | Оценка осведомлённости персонала о политике безопасности и об ответственности |
| 6 | Имеется ли у Вас план действий на случай происшествий, связанных с информационной безопасностью, в Вашей системе защиты и управления? | ДА, НЕТ, ПЛАНИРУЕТСЯ к концу 2015 года, НЕ ЗНАЮ | Оценка знания персоналом служб защиты и управления своих обязанностей по ликвидации последствий происшествий в информационной среде |
| 7 | Контролируете ли Вы персональный доступ и использование сотрудниками элементов системы защиты и управления? | ДА, НЕТ, ПЛАНИРУЕТСЯ к концу 2015 года, НЕ ЗНАЮ | Оценка отношения организации, эксплуатирующей системы защиты и управления, к контролю доступа и полномочий. |
| 8 | При устранении неисправностей, связанных с информационной безопасностью, проверяете ли Вы исправления, вносимые в систему защиты и управления, до их применения? | ДА, НЕТ, ПЛАНИРУЕТСЯ к концу 2015 года, НЕ ЗНАЮ | Оценка доверия организаций, эксплуатирующих системы защиты и управления, к исправлениям, которые они получают от производителей компонентов этих систем |
| 9 | Располагаете ли Вы необходимыми средствами контроля за системой защиты и управления, позволяющими выявлять факты нарушения безопасности? | ДА, НЕТ, ПЛАНИРУЕТСЯ к концу 2015 года | |
| 10 | Пользуетесь ли Вы тестовыми | ДА, НЕТ, ПЛАНИРУЕТСЯ к | |

| Номер вопроса | Вопрос | Варианты ответа | Цель вопроса |
|---|---|---|---|
| | программами или оценочными листами для оценки происшествий, связанных с нарушением информационной безопасности? | концу 2015 года, НЕ ЗНАЮ | |
| 11 | Если Вы ответили ДА на 10 вопрос, то автоматизированы ли эти оценочные листы? | ДА, НЕТ | |
| 12 | Составьте свой краткий список мероприятий в области информационной безопасности, необходимых для Вашей системы защиты и управления | Список | Сбор информации, необходимой для упорядочивания мероприятий по информационной безопасности для систем защиты и управления |
| 13 | Какое мероприятие в области информационной безопасности является приоритетным (основным) для Вашей системы защиты и управления? | Приоритетное (основное) решение | |
| 14 | Какое из мероприятий по информационной безопасности является наиболее сложным для инженеров и технического персонала системы защиты и управления в эксплуатации и организации? | Наиболее труднореализуемое мероприятие | |
| 15 | Располагаете ли Вы техническими и организационными возможностями для организации ролевого управления доступом в системах защиты и управления? | ДА, НЕТ, ПЛАНИРУЕТСЯ к концу 2015 года, НЕ ЗНАЮ | |
| 16 | Привлекаете ли Вы сторонние компании для организации ролевого управления доступом в системах защиты и управления? | ДА, НЕТ, ПЛАНИРУЕТСЯ к концу 2015 года, НЕ ЗНАЮ | |
| 17 | Каким образом вы обеспечиваете ролевое управление доступом в системах защиты и управления? | Опишите в нескольких предложениях Ваш подход | |
| 18 | Разрешено ли Вашим сотрудникам использовать их собственные электронные | для технического обслуживания, для настройки элементов систем защиты и | Сбор информации, необходимой для оценки |

| Номер вопроса | Вопрос | Варианты ответа | Цель вопроса |
|---|---|---|---|
| | устройства (например, личный флэш-накопитель, смартфон, планшет и т.д.) для технического обслуживания или настройки элементов системы защиты и управления? | управления, ОБА ВАРИАНТА, НИ ОДИН ИЗ ВАРИАНТОВ | степени использования персональных электронных устройств для технического обслуживания и настройки элементов систем защиты и управления |
| 19 | Планируете ли Вы разрешить Вашим сотрудникам использовать их собственные электронные устройства (например, личный флэш-накопитель, смартфон, планшет и т.д.) для технического обслуживания или настройки элементов системы защиты и управления? | для технического обслуживания, для настройки элементов системы защиты и управления, ОБА ВАРИАНТА, НИ ОДИН ИЗ ВАРИАНТОВ, НЕ ЗНАЮ | |
| 20 | Осуществляете ли Вы поддержку программ для обслуживания оборудования системы защиты и управления, загружаемых на персональные электронные устройства Ваших сотрудников? | программ для технического обслуживания, программ для настройки элементов системы защиты и управления, ОБА ВАРИАНТА, НИ ОДИН ИЗ ВАРИАНТОВ, НЕ ЗНАЮ | |
| 21 | Оцените уровень использования персональных электронных устройств Вашими сотрудниками для обслуживания оборудования системы защиты и управления. | Техническое обслуживание оборудования системы защиты и управления: 0%, 25%, 50%, 75% или больше<br>Настройка элементов системы защиты и управления: 0%, 25%, 50%, 75% или больше | |
| 22 | Внедряете ли Вы правила разграничения доступа и шифрование для персональных электронных устройств Ваших сотрудников при использовании этих устройств для: | Технического обслуживания, настройки элементов РЗ и управления, ОБА ВАРИАНТА, НИ ОДИН ИЗ ВАРИАНТОВ, НЕ ЗНАЮ | |
| 23 | Позволяете ли Вы специалистам технической поддержки из сторонних компаний использовать их собственные электронные устройства (например, личный флэш- | для технического обслуживания, для настройки элементов системы защиты и управления, ОБА ВАРИАНТА, НИ ОДИН ИЗ ВАРИАНТОВ, НЕ ЗНАЮ | |

| Номер вопроса | Вопрос | Варианты ответа | Цель вопроса |
|---|---|---|---|
| | накопитель, смартфон, планшет и т.д.) для технического обслуживания или настройки элементов системы защиты и управления? | | |
| 24 | Планируете ли Вы разрешить специалистам технической поддержки из сторонних компаний использовать их собственные электронные устройства (например, личный флэш-накопитель, смартфон, планшет и т.д.) для технического обслуживания или настройки элементов системы защиты и управления? | для технического обслуживания, для настройки элементов системы защиты и управления, ОБА ВАРИАНТА, НИ ОДИН ИЗ ВАРИАНТОВ, НЕ ЗНАЮ | |
| 25 | Поддерживаете ли Вы программы для обслуживания оборудования системы защиты и управления, загружаемые на персональные электронные устройства специалистов технической поддержки из сторонних компаний? | программы для технического обслуживания, программы для настройки элементов системы защиты и управления, ОБА ВАРИАНТА, НИ ОДИН ИЗ ВАРИАНТОВ, НЕ ЗНАЮ | |
| 26 | Оцените уровень использования персональных электронных устройств специалистами технической поддержки из сторонних компаний для обслуживания оборудования системы защиты и управления. | Техническое обслуживание оборудования системы защиты и управления: 0%, 25%, 50%, 75% или больше<br>Настройка элементов системы защиты и управления: 0%, 25%, 50%, 75% или больше | |
| 27 | Внедряете ли Вы правила разграничения доступа и шифрование для персональных электронных устройств специалистов технической поддержки из сторонних компаний при использовании этих устройств для: | Технического обслуживания, настройки элементов системы защиты и управления, ОБА ВАРИАНТА, НИ ОДИН ИЗ ВАРИАНТОВ, НЕ ЗНАЮ | |
| 28 | Выберите из следующего списка основной фактор, | • Стоимость обслуживания и эксплуатации надёжной системы безопасности<br>• Достаточно тех мер и | Сбор информации, необходимой для |

| Номер вопроса | Вопрос | Варианты ответа | Цель вопроса |
|---|---|---|---|
| | ограничивающий внедрение строгих норм и мероприятий в области безопасности для систем защиты и управления (выберите только один). | средств безопасности, которые предлагает наше ИТ подразделение<br>• Плохая совместимость между элементами системы защиты и управления<br>• Невозможно внедрить надёжные механизмы в элементы системы защиты и управления | определения основных препятствий для внедрения и эксплуатации надёжных программ защиты |
| 29 | Использовали ли Вы требования каких-либо нормативных документов для создания собственных норм и мероприятий по информационной безопасности для системы защиты и управления? Если да, то какие нормативные требования были использованы? | ДА, НЕТ | Сбор информации, необходимой для упорядочивания нормативных требований, которые непосредственно влияют на нормы и мероприятия по информационной безопасности в системах защиты и управления |
| 30 | Если Вы ответили НЕТ на 29 вопрос, то какие источники вы использовали при составлении собственных норм по информационной безопасности? | • Служебные руководящие указания<br>• Общепринятые отраслевые руководящие указания<br>• Рекомендации профессиональных объединений<br>• Рекомендации для персонала систем защиты и управления | |
| 31 | Пожалуйста, оставьте комментарий, объясняющий Ваши ответы (по желанию) | Свободная форма | Разъяснения к данной анкете. |

## D.2.3 Анализ результатов исследования

### D.2.3.1 Введение

Компания Newton-Evans опубликовала результаты исследования в докладе, который находится в открытом доступе [53]. Данная техническая брошюра использует результаты этого исследование для того, чтобы обратить внимание на некоторые специфические вопросы.

### D.2.3.2 Получают ли инженеры, эксплуатирующие системы защиты и управления, необходимую начальную подготовку для обнаружения информационных атак

Для инженеров систем защиты и управления специально проводится начальная подготовка, которая формирует основу для борьбы с информационными атаками, представляющими значительную угрозу для надёжности и возможности осуществления энергоснабжения.

В целом, существует в основном равное разделение между теми энергокомпаниями, которые проводят обучение по вопросам информационной безопасности (35%), теми, которые не проводят (33%) и теми, кто не занимается этим в настоящее время, но планирует начать к концу 2015 года

(32%). При этом, среди североамериканских энергокомпаний почти половина проводят обучение по вопросам информационной безопасности в настоящее время, в то время как среди международных энергокомпаний таким обучением занимается только четверть. Совокупность тех компаний, которые уже занимаются обучением и тех, которые только планируют начать, составляет 65%, что неплохо для начала, однако остаётся ещё много возможностей для улучшения.

Обучение должно быть согласовано с той деятельностью, которую выполняют инженеры систем защиты и управления. Если оно не соответствует их деятельности, уровень информационной безопасности электроэнергетических компаний значительно снижается. В целом, менее половины респондентов проводят обучение по информационной безопасности, связанное с должностными обязанностями своего персонала. Тем не менее, в Северной Америке 48% опрошенных отметили, что проводят такое обучение.

Большинство опрошенных оценивают свою деятельность по обучению персонала вопросам информационной безопасности как “средне” и “плохо”, меньшее количество международных энергокомпаний оценили своё обучение как “хорошее” или “полноценное”. В одной пятой части североамериканских энергокомпаний считают, что их обучение информационной безопасности “очень хорошее”.

Очень немногие опрошенные должностные лица (8%) считают, что их подготовка по информационной безопасности “хороша и без всяких улучшений”. Североамериканские энергокомпании отмечают возможности для “некоторого улучшения”, в то время как международные компании ответили, что “Да, довольно много” улучшений могло бы быть сделано.

Сорок четыре процента североамериканских энергокомпаний сообщили, что имеют правила допустимого использования сети, подписанные их персоналом системы защиты и управления, 30% международных энергокомпаний отметили то же самое. Пять из восьми владельцев североамериканских энергокомпаний ответили на этот вопрос “Да”.

Приблизительно половина всех опрошенных энергокомпаний КОНТРОЛИРУЕТ персональный доступ работников к элементам систем защиты и управления. Почти четверть респондентов, не имеющих такого контроля, планируют ввести его к концу 2015 года.

Из ответов становится ясно, что значительное число элементов программ обучения электроэнергетических компаний в сфере безопасности нуждается в улучшении.

### D.2.3.3 Располагают ли инженеры систем защиты и управления необходимыми инструментами для борьбы с информационными атаками?

Сорок два процента североамериканских и 22% международных энергокомпаний отметили наличие плана реагирования на происшествия в своих системах защиты и управления.

Более половины опрошенных в Северной Америке энергокомпаний сообщили, что они располагают необходимыми средствами контроля для отслеживания случаев нарушения безопасности в системе защиты и управления. Другие 24 % отметили, что, хотя они и не имеют таких средств контроля на данный момент, эти средства появятся в наличии к концу 2015 года. Только 1 из 4 международных энергокомпаний в выборке считает, что имеет в наличии необходимые средства контроля для отслеживания случаев нарушения безопасности.

Около половины энергокомпаний в выборке не используют тестовые программы или оценочные листы для анализа происшествий, связанных с нарушением информационной безопасности. Тридцать процентов международных и двадцать процентов североамериканских энергокомпаний в выборке планируют начать их использование к концу 2015 года. Только 7 из более 60 энергокомпаний в выборке ответили, что используют оценочные листы для оценки происшествий, связанных с нарушением информационной безопасности. Из этих семи только две сообщили, что они автоматизировали эти оценочные листы.

Учитывая повышенное внимание к вопросам безопасности, необходимость защиты важных

объектов инфраструктуры электроэнергетических компаний, а также их бюджетное финансирование в Северной Америке и Евросоюзе, недостаток сравнительного анализа случаев нарушения безопасности является удивительным. Трудно понять, как электроэнергетические компании могут эффективно управлять программами по обеспечению информационной безопасности без должного отслеживания и анализа происшествий.

### D.2.3.4 В достаточной ли мере инженеры систем защиты и управления проверяют исправления, вносимые в системы?

В целом, примерно одна треть энергокомпаний испытывает исправления, одна треть – не испытывает и почти одна треть не занимается этим в настоящее время, но планирует начать к концу 2015 года.

Хотя примерно две трети опрошенных электроэнергетических компаний и планируют начать испытывать исправления, вносимые в системы безопасности, к концу 2015 года, фактически остаётся треть компаний, которые не собираются этим заниматься. К сожалению, исследование не содержало дополнительных вопросов, которые помогли бы понять проблемы и выявить ограничивающие факторы, связанные с применением исправлений. Эта проблема нуждается в дальнейшем исследовании.

### D.2.3.5 Какие решения необходимы по мнению инженеров систем защиты и управления

Пятьдесят один из шестидесяти трёх опрошенных респондентов предоставили письменный ответ на вопрос “Составьте свой краткий список мероприятий в области информационной безопасности, необходимых для Вашей системы защиты и управления”. В целях проведения анализа ответы сгруппированы на основе сочетаний использованных слов и подразумеваемого смысла. Хотя все написанные ответы содержали веские проблемы и решения, связанные с обеспечением информационной безопасности, около половины написанных ответов были слишком уникальны и разнообразны, чтобы быть отнесёнными к какой-либо категории (все ответы приведены согласно своему номеру на следующих нескольких страницах).

Больше половины респондентов (55%) отметили необходимость ограничения доступа и возможности подключения посредством нескольких способов: разделение/сегментация сети, управление доступом, использование закрытых сетей, запрет подключения к Интернету, ограничение физического доступа или ограничение числа точек доступа в целом (физическое или электронное). Тридцать семь процентов упоминали некоторые способы ведения журнала доступа или сетевого мониторинга, такие как IDS (система обнаружения несанкционированного доступа). Только 4% упомянули шифрование, которое следует дальше в кратком списке необходимых мероприятий по информационной безопасности.

Аналогично данному вопросу, многие респонденты (12) упомянули вариант “ограничения или контроля доступа и возможности подключения” как наиболее предпочтительное решение по информационной безопасности. Также было четыре упоминания о межсетевых экранах и одно об антивирусных программах, однако 4 респондента также отметили, что не существует одного приоритетного решения по информационной безопасности – все они в равной степени важны либо существует групповое приоритетное решение.

### D.2.3.6 В чём заключаются ограничения по использованию персональных электронных устройств для технического обслуживания или настройки элементов систем защиты и управления?

Больше, чем три четверти опрошенных НЕ разрешают своим сотрудникам использовать персональные электронные устройства как для технического обслуживания, так и для настройки элементов систем защиты и управления.

Из тех сорока восьми энергокомпаний, которые не позволяют своим сотрудникам использовать персональные электронные устройства для эксплуатации или настройки элементов, только две планируют позволить такое использование для эксплуатации устройств защиты и управления и одна энергокомпания планирует согласиться на использование персональных электронных

устройств для настройки элементов систем защиты и управления.

Примерно пятая часть респондентов отметили, что позволяют сторонним компаниям технической поддержки использовать их собственные персональные электронные устройства при эксплуатации систем защиты и управления, и почти четверть позволяют им использовать персональные электронные устройства для настройки компонентов этих систем.

Семь процентов опрошенных компаний сообщили, что они осуществляют поддержку программ, загружаемых на персональные электронные устройства специалистов технической поддержки из сторонних компаний, для эксплуатации систем защиты и управления, и одиннадцать процентов указали, что они занимаются поддержкой программ для настройки компонентов этих систем. Поддержка обоих видов таких программ среди международных энергокомпаний распространена немного больше, чем среди североамериканских.

Пятьдесят пять процентов всех опрошенных энергокомпаний полагают, что никто из работающих с ними специалистов из сторонних компаний не использует персональные электронные устройства для эксплуатации систем защиты и управления. Девятнадцать процентов не уверены и восемнадцать процентов отметили, что примерно четверть работающих с ними специалистов сторонних компаний, которых они нанимают, используют персональные электронные устройства при эксплуатации систем защиты и управления.

Ограничение использования персональных электронных устройств в некоторой степени может сбить с толку. Электроэнергетические компании однозначно не рекомендуют использование персональных электронных устройств своим работниками, но они не стремятся накладывать такие же ограничения на специалистов сторонних компаний.

**D.2.3.7 Как требования нормативных документов влияют на эксплуатацию систем защиты и управления?**

Влияние требований нормативных документов на политику в области информационной безопасности систем защиты и управления больше сказывается на североамериканских энергокомпаниях, чем на международных. Восемьдесят девять процентов международных энергокомпаний ответили “НЕТ” на данный вопрос, в то время как среди североамериканских компаний “НЕТ” ответили только 40%.

Многие североамериканские энергокомпании ссылались на требования Североамериканской корпорации по обеспечению надёжности электроэнергетических систем (NERC) и Федеральной комиссии по регулированию в энергетике (FERC) как на необходимые или оказывающие значительное влияние на их политику в отношении информационной безопасности систем защиты и управления. Одна из международных энергокомпаний упомянула нормы безопасности международной организации стандартизации (ISO).

Наибольшая часть данных по этому вопросу пришла от 32 международных компаний, а также от 10 североамериканских энергокомпаний, которые ответили “НЕТ” (то есть, не на основе нормативных требований) на вопрос “Использовали ли Вы требования каких-либо нормативных документов для создания собственных норм и мероприятий по информационной безопасности для системы защиты и управления?”

Руководящие положения ИТ департамента в совокупности с руководящими положениями индустрии и энергокомпаний оказывают наибольшее влияние на политику в области информационной безопасности. Профессиональные ассоциации имеют больше влияния на политику информационной безопасности международных компаний, чем североамериканских.

**D.2.3.8 Выводы, полученные из анализа результатов исследования**

Объединённая рабочая группа CIGRE JWG B5-D2.46 использовала данное исследование и результаты анализа полученных ответов для того, чтобы скорректировать направление развития этой технической брошюры. В целях дополнения результатов опроса, члены объединённой рабочей группы представили научные доклады на различных открытых площадках, конференциях

и проектных совещаниях для того, чтобы получить новые мнения и объяснения этих вопросов. Объединённая рабочая группа использовала эти мнения и объяснения для улучшения данной технической брошюры.

Вот несколько важных выводов, полученных с помощью этих результатов.

a) Учитывая повышенное внимание к вопросам безопасности и бюджетный характер финансирования в Северное Америке и Евросоюзе, ответы электроэнергетических компаний являются довольно удручающими. Недостаток автоматизированных тестовых программ для анализа нарушений безопасности вызывает наибольшее беспокойство, так как это ухудшает эффективность управления стратегией обеспечения безопасности.

b) Несмотря на то, что электроэнергетические компании уже внедряют обучение по вопросам безопасности, в этой сфере все ещё остаётся много возможностей для улучшения. В первую очередь, обучение, связанное с должностными обязанностями, улучшает точность выполнения и лёгкость восприятия функций информационной безопасности.

c) Плохо реализован (в лучшем случае) контроль за программными исправлениями в области безопасности. В начале 2015 года международное общество автоматизации (ISA) выпустит для ознакомления технический отчёт международной электротехнической комиссии IEC/TR 62443-2-3. В будущем комитет ISA99 планирует преобразовать этот технический отчёт в техническое требование или стандарт. Электроэнергетическим компаниям предложено изучить и прокомментировать части 2-3 в целях улучшения их соответствия своей организационной среде и техническим ограничениям.

d) Использование персональных электронных устройств позволяет экономить средства и является настолько коммерчески привлекательным, что в конце концов электроэнергетические компании будут вынуждены снять свои ограничения по поводу возможности использования таких устройств при работе с системами и оборудованием защиты и управления. Это справедливо в отношении их использования как для удалённого доступа, так и для локального доступа в пределах подстанций.

# Приложение E
# Безопасная адаптация персональных устройств к системам защиты и управления и их составляющим

## E.1 Будущее близко

**Рисунок E-11 BYOD - планшет**

По правде говоря, специалистам системы защиты и управления и оперативно-выездным техникам нравятся эти мобильные устройства, потому что можно использовать свои собственные. Планшетные устройства способны конфигурировать и поддерживать настройки интеллектуальных электронных устройств (ИЭУ) особой важности. Они подключаются к ИЭУ посредством беспроводной связи или через соединение по USB-кабелю. Они обладают производительной мощностью и объемами хранимых данных, достаточными для опроса ИЭУ и определения подходящего момента для изменения настроек. Если находящемуся на подстанции специалисту требуются дополнительные сведения, беспроводная сеть позволяет загрузить эти данные с интернет-сервера. Кроме того, если доступ к оперативной сети электроэнергетической системы открыт и разрешен, возможна загрузка данных с рабочего сервера или сервера архивных данных.

## E.2 Риски, которыми необходимо управлять

В первую очередь ОРГ обеспокоена внутренней угрозой, которая создается при использовании инженерами релейной защиты и управления или оперативно-выездными техниками (пользователями) их собственных устройств (BYOD, Bring Your Own Device – концепция использования собственных устройств сотрудников), таких, как планшетное устройство, показанное на рисунке E-11. В этом случае пользователь хорошо осведомлен о системе защиты и управления, её настройках и функциональных показателях. Некомпетентный пользователь способен причинить существенный вред.

Инженеры релейной защиты и управления и оперативно-выездные техники работают на инжиниринговые компании или обслуживающие организации, которые ответственны за минимизацию рисков, касающихся информационной безопасности общественной сети и устройств системы защиты и управления. Чтобы эффективно управлять рисками, они должны обладать средствами определения и оценки возможности риска или, в противном случае, должны блокировать доступ и возможность использования BYOD или предусмотреть для них специальные защитные меры. ОРГ рассмотрела решения задачи управления информационной безопасностью, учитывающие пользователей BYODs.

## E.3 Безопасное сопряжение персональных устройств

Чтобы безопасно присоединить любое персональное устройство к системе защиты и управления, ОРГ обозначила три требования особой важности: (1) полная видимость сети, (2) изучение и оперативная проверка устройства и (3) обеспечение безопасного подключения к сети. Реализация этих требований должна позволить ответственным организациям определять, кто использует персональное устройство, персональное устройство какого типа используется, где оно используется и когда. Должны быть реализованы два принципа управления.

а) Чтобы получить доступ к системе защиты и управления при помощи персонального устройства, пользователи должны пройти авторизацию после создания аккаунта и регистрации своего персонального устройства.

б) Современные системы защиты и управления должны иметь закрытый доступ, для посетителей должны быть введены специальные параметры доступа: ограниченный доступ,

предусматривающий только чтение, или полный доступ, разрешающий чтение/запись.

Своевременное реагирование на неавторизованные сетевые подключения подразумевает непрерывный автоматический мониторинг использования персональных устройств. Способность различать конкретное персональное устройство вместе с пользователем и визуализировать, где и когда была зафиксирована активность, крайне важна. Наконец, структура системы информационной безопасности должна быть довольно гибкой, так как необходимость использования персональных устройств значительно вырастет в ближайшие 10 лет.

# Приложение F
# Обеспечение безопасности систем защиты и управления от атак межсайтового скриптинга

## F.1 Межоперационные системы защиты и управления уязвимы перед атаками межсайтового скриптинга (XSS, Cross-Site Scripting)

Межоперационная совместимость – это основополагающее требование, предъявляемое к современным системам защиты, в частности к тем, что руководствуются положениями МЭК 61850. Браузеры приложений не ограничивают возможность ввода данных пользователем с целью обеспечить операционную совместимость между средствами конфигурирования и элементами системы защиты и управления. Пользуясь этим, злоумышленники могут ввести вредоносный код, вызывая тем самым непредусмотренные выполнения скрипта браузерами других клиентов. ОРГ изучила две проблемы информационной безопасности релейной защиты и управления:

в) Обнаружив пути ввода вредоносного кода на страницах браузера приложения, злоумышленник способен получить к чувствительным настройкам релейной защиты и управления доступ с повышенными привилегиями. Таким образом, XSS выступает как частный случай внедрения кода.
г) Атаки межсайтового скриптинга также представляют опасность, потому что злоумышленник может использовать в своих целях уязвимость браузеров, заключающуюся в требовании идентификации пользователя для предоставления доступа. Эти уязвимости известны как "пост-идентификационные атаки межсайтового скриптинга".

### F.1.1 Средства защиты от XSS

В целом средства защиты от XSS делятся на четыре типа: разработка защитных кодов, тестирование XSS, обнаружение уязвимостей и предотвращение атак в режиме реального времени. Каждое из этих средств имеет как преимущества, так и недостатки.

Обычно на подстанциях, оснащенных высокоавтоматизированными системами, ответственность за информационную безопасность релейной защиты и управления разделена между тремя специалистами: разработчик элементов релейной защиты и управления, инженер релейной защиты и управления и инженер информационной сети. В таблице F-10 приведена степень вовлеченности каждого специалиста в обеспечении шести рекомендуемых методов обеспечения безопасности системы защиты и управления.
Тестирование и оценивание XSS – это узкоспециализированный навык. Руководство электроэнергетических систем обычно обращается за технической поддержкой для инженеров релейной защиты и управления и инженеров информационной сети с целью обеспечения независимой проверки и подтверждения корректности схем обеспечения информационной безопасности.

### F.1.2 Определение степени надежности настроек системы защиты и управления с целью обнаружить уязвимости перед атаками межсайтового скриптинга в системной конфигурации и служебных приложениях

Разработчики элементов системы защиты и управления должны продемонстрировать в своих заводских приёмосдаточных испытаниях (FAT) и приемочных испытаниях на месте (SAT) способность поддерживать контроль защищенного доступа и использовать права доступа, предусмотренные в их браузерах приложений для конфигурирования и поддержания элементов системы защиты и управления и устройств общественных сетей. FAT и SAT планы и процедуры должны точно описывать методы, которые должны быть использованы для демонстрации, и ожидаемые результаты, потенциально применимые для поддержания надежности системы защиты и управления.

Инженер системы защиты и управления и инженер информационной сети должны изучить и одобрить FAT и SAT планы и процедуры. Обновленные планы и процедуры отражают изменения в

элементах системы защиты и управления и сетевых устройствах. Перед внедрением центральная служба качества путем лабораторных испытаний обеспечивает высшую степень конфиденциальности своей защитной конфигурации.

### F.1.3 Тестирование информационной безопасности системы защиты и управления на наличие ошибок с целью оценить эффективность схем минимизации вреда от атак межсайтового скриптинга

Разработчики элементов релейной защиты и управления должны продемонстрировать в своих заводских приёмосдаточных испытаниях (FAT) и приемочных испытаниях на месте (SAT) способность обнаруживать и минимизировать последствия от атак межсайтового скриптинга. FAT и SAT планы и процедуры должны точно описывать используемые алгоритмы.

Инженер релейной защиты и управления и инженер информационной сети должны определить все требования к функциям обнаружения и минимизации вреда от повреждений в результате кибератак, возложенным на элементы системы защиты и управления и сетевые устройства соответственно. Перед внедрением осуществляется тестирование изменений в этих схемах обнаружения и минимизации вреда в центральной лаборатории службы качества.

### F.1.4 Проведение анализа статических характеристик для подтверждения отсутствия уязвимостей

Анализ статических характеристик служит для подтверждения отсутствия уязвимостей, но он также имеет свойство вызывать ложное распознавание сигнала. Инженеры релейной защиты и управления и инженеры информационной сети должны в комплексе рассматривать статические и динамические характеристики с целью повышения точности.

Технологии анализа технических характеристик определяют сомнительные вводы, разрешенные внешними источниками данных, отслеживают поток сомнительных данных и проверяют, доступны ли рабочие операторы и операторы вывода элементов релейной защиты и управления и сетевых устройств. В то же время, они не могут проверить корректность проверочных функций ввода и, напротив, обычно допускают, что необработанные или неизвестные функции возвращают небезопасные данные. Эти методики также упускают уязвимости перед XSS атаками, так как их целью не являются клиентские скрипты, используемые конфигурационными и профилактическими средствами браузеров.

Разработчики элементов релейной защиты и управления должны представить анализ статических характеристик в среде выполнения программ на агрегатном уровне и на уровне заводских приёмосдаточных испытаний. Повторный анализ элементов релейной защиты и управления в центральной лаборатории службы качества перед началом полевых испытаний предоставляет возможность сравнить полученные результаты с результатами тестов в среде выполнения программ. Подобную процедуру проводят также и для сетевых устройств.

### F.1.5 Проведение анализа динамических характеристик для дополнения анализа статических характеристик

Для компенсации неспособности статического анализа определить корректность проверочных функций проводят динамический анализ. Шар и Куан Тан заключили, что “комбинированный статический и динамический анализ может выявить точные направления атак и тем самым избежать ложных распознаваний сигнала; это также позволяет полностью автоматизировать средство генерации тестовых сценариев” – см. [54]. Кроме того, они отметили, что текущий уровень реализации охватывает только серверные сценарии; клиентские сценарии нуждаются в дальнейшем анализе.

Ввиду этих ограничений разработчики элементов релейной защиты и управления должны поддерживать инициативу центральной лаборатории службы качества, а именно: обеспечить промежуточную обходную процедуру и определить требования к предусмотренной возможности совершенствования изделий (ПВС) для последующих нововведений.

### F.1.6 Предотвращение атак межсайтового скриптинга на стороне сервера системы защиты и управления

Обеспечение безопасности элементов релейной защиты от атак межсайтового скриптинга на стороне сервера требует от пользователей определить исходные условия чувствительных функций и конечные условия проверочных функций. Во время выполнения инструментальные защиты проверяют соблюдение установленных для пользователей условий.

Другой подход заключается в использовании динамических, следящих за сомнительными данными механизмов для контроля потока входных данных в режиме реального времени. Их наличие гарантирует, что эти вводы синтаксически ограничены (содержат только буквенные значения) и не содержат небезопасных данных, определенных пользовательской политикой безопасности.

В основном, защита на стороне сервера может предотвратить все атаки межсайтового скриптинга, так как она проверяет важные текущие значения входных данных, а оценка необходима. Тем не менее, она испытывает потребность в технических средствах кодирования для обеспечения динамического мониторинга и установки дополнительных объектных структур, а также, в некоторых случаях, определяемых пользователем мер безопасности, и оба эти процесса могут быть весьма трудоемкими.

Разработчики элементов системы защиты и управления должны проводить центральный анализ по предотвращению атак со стороны сервера для обеспечения промежуточной обходной процедуры и ввода требований ПВС для последующих нововведений. Инженеры системы защиты и управления и инженеры информационной сети должны определить потенциально уязвимые ключевые элементы системы защиты и управления и элементы общественной сети и снабдить их защитой в режиме реального времени для проверки соответствия установленным требованиям.

### F.1.7 Предотвращение атак межсайтового скриптинга на стороне пользователя систем защиты и управления

Использование правил фильтрации позволяет предотвращать атаки межсайтового скриптинга на стороне пользователя релейной защиты и управления за счет разрешения или блокировки соединений к элементам релейной защиты и управления или элементам сети. Правила фильтрации представляют собой белые или черные списки, определенные пользователями. Когда ненадежный элемент релейной защиты и управления или компонент сети посылает запрос пользователю релейной защиты и управления (терминал or BYOD), шлюз безопасности немедленно предупреждает клиента, который решает разрешить или запретить соединение, и запоминает действие пользователя для будущего использования. Превентивные меры на стороне пользователя представляют клиентам собственный уровень защиты, поэтому у них нет необходимости полностью полагаться на обеспечение безопасности релейной защиты и управления или защиту элементов сетевых приложений. Основной недостаток такой системы в том, что она нуждается в пользовательских действиях даже в случае, если соединение нарушает правила фильтрации.

Разработчики элементов релейной защиты и управления должны проводить централизованный анализ превентивных мер на стороне пользователя системы защиты и управления для обеспечения промежуточной обходной процедуры и ввода требований ПВС для последующих нововведений. Инженеры релейной защиты и управления и инженеры информационной сети должны определить потенциально уязвимые ключевые элементы системы защиты и управления и элементы общественной сети снабдить их защитой в режиме реального времени для проверки соответствия установленным требованиям.

## F.2 Предотвращение XSS требует участия всех заинтересованных сторон

Обычно организации, контролирующие системы релейной защиты и управления, и сетевые компании не располагают специальными технологиями по предотвращению XSS. Разработчики элементов релейной защиты и управления будут разрабатывать возможности, необходимые для защиты от атак межсайтового скриптинга, если поймут и реализуют в своих продуктах и службах требования по информационной безопасности. Они являются заинтересованной стороной, но

нуждаются в помощи.

Таблица F-10 описывает степени участия в обеспечении безопасности систем защиты и управления от атак межсайтового скриптинга. Специалисты в области энергетики и в области релейной защиты и управления должны заключить соглашение со специалистами узкого профиля (SMEs), занимающимися атаками межсайтового скриптинга, и рассматривать их как полноценного участника совещательной группы заинтересованных сторон (SAG).

**Таблица F-10 Степень участия в обеспечении безопасности систем защиты и управления при атаках межсайтового скриптинга**

| Метод | Степень участия | | |
|---|---|---|---|
| | **Разработчик элементов релейной защиты и управления** | **Инженер релейной защиты и управления** | **Инженер информационной сети** |
| **Проверка корректности настроек защиты и управления** | планы и процедуры испытаний элементов | технический осмотр и право утверждать решения касательно элементов систем защиты и управления | технический осмотр и право утверждать решения касательно элементов сети |
| **Тестирование системы информационной безопасности на наличие ошибок** | внедрение в элементы алгоритмов обнаружения нарушений информационной безопасности и уменьшения отрицательных последствий | устанавливает требования к функциям обнаружения нарушений информационной безопасности и уменьшения отрицательных последствий с точки зрения релейной защиты и управления | устанавливает сетевые требования к функциям обнаружения нарушений информационной безопасности и уменьшения отрицательных последствий |
| **Статический анализ** | представляет анализ статических характеристик в среде выполнения программ на агрегатном уровне и на уровне «сухого прогона» | представляет статический анализ элементов релейной защиты и управления в центральной лаборатории службы качества перед началом полевых испытаний | представляет статический анализ элементов сети в центральной лаборатории службы качества перед началом полевых испытаний |
| **Динамический анализ**[20] | поддерживает инициативу центральной лаборатории службы качества обеспечить промежуточную обходную процедуру и ввести требование предусмотренной возможности совершенствования изделий (ПВС) для последующих нововведений | представляет динамический анализ элементов релейной защиты и управления в центральной лаборатории службы качества перед началом полевых испытаний | представляет динамический анализ элементов сети в центральной лаборатории службы качества перед началом полевых испытаний |

[20] Динамический анализ проводят в лаборатории службы качества с использованием реальных данных и направлений виртуальных атак, методов очистки системы защиты с целью предотвращения нарушения операционных параметров и функций релейной защиты и управления.

| Метод | Степень участия | | |
|---|---|---|---|
| | **Разработчик элементов релейной защиты и управления** | **Инженер релейной защиты и управления** | **Инженер информационной сети** |
| **Превентивные меры на стороне сервера** | проведение центрального анализа предотвращения атак со стороны сервера для обеспечения промежуточной обходной процедуры и ввода требований ПВС для последующих нововведений | определение потенциально уязвимых ключевых элементов релейной защиты и управления и снабжение их защитой в режиме реального времени для проверки соответствия установленным требованиям | определение потенциально уязвимых ключевых элементов общественной сети и снабжение их защитой в режиме реального времени для проверки соответствия установленным требованиям |
| **Превентивные меры на стороне пользователя** | проведение централизованного анализа превентивных мер на стороне пользователя релейной защиты и управления для обеспечения промежуточной обходной процедуры и ввода требований ПВС для последующих нововведений | определение сомнительных внешних интерфейсов к ключевым элементам релейной защиты и управления и снабжение их защитой в режиме реального времени для проверки соответствия установленным требованиям | определение сомнительных внешних интерфейсов к ключевым элементам общественной сети и снабжение их защитой в режиме реального времени для проверки соответствия установленным требованиям |

# Приложение G
# Криптографические функции хэширования

## G.1 Функции хэширования используются для обеспечения безопасности релейной защиты и управления

Волкер и остальные[55] заключили, что функции хэширования являются одним из фундаментальных криптографических строительных блоков и по важности превосходят даже функции шифрования. Например, цифровые отпечатки и схемы фиксации, такие как подтверждение подлинности сообщений и генерация случайных чисел, наряду со схемами электронной подписи, потоковыми шифрами и случайными выборками используют функции хэширования. МЭК/TS 62351 устанавливает хэш-требования для протоколов, в том числе СПС, МЭК 61850 и МЭК 60870-5 и их производные.

Хотя теория, структура и реализация функций хэширования совершенно не рассматриваются в этой технической брошюре, инженеры релейной защиты и управления и инженеры информационной сети должны иметь общее представление о механизмах хэширования, поскольку эти механизмы относятся к требованиям безопасности в их сфере ответственности.

## G.2 Основные приложения системы защиты и управления, использующие функции хэширования

Далее представлен список, содержащий шесть типов функций хэширования.

**Цифровые отпечатки**: используются для представления структур цифровых данных, их профиль представления - это их «отпечатки».

**Электронно-цифровые подписи**: расширяют цифровые отпечатки зашифровыванием значения хэша структуры данных персональным ключом.

**Подтверждение подлинности сообщений**: используется с секретным паролем для идентификации сообщения.

**Псевдослучайная генерация чисел**: используется для построения генератора случайных чисел с применением пароля, называемого зерном, для вычисления значения хэша, когда каждая хэш-сумма представляет собой случайное число.

**Потоковые шифры**: зашифровывает сообщение, используя хэш.

**Случайные выборки**: используют специальный генератор случайных чисел для рандомизации зашифровывания публичных и персональных паролей.

Для идентификации уровня приложения, МЭК/TS 62351-4 (2005) определяет использование алгоритма безопасного хэширования SHA-1 в целях подписания ассоциативных запросов. SHA-2 заменит SHA-1 в следующем издании технической документации.

Эта операция независима от алгоритма уточнения подписи, используемого для установления подлинности документов или в целях аутентификации узлов на транспортном уровне (TLS). МЭК/TS 62351 выступает за использование конкретных алгоритмов шифрования и содержит рекомендации для тех алгоритмов, которые могут быть использованы на уровне TLS. Тем не менее, техническая документация не регламентирует аутентификацию и зашифровывание на уровне TLS. Она лишь предлагает разумный выбор шифров, реализованных открытым протоколом защиты информации (OpenSSL).

МЭК/TS 62351-6 определяет требования к алгоритму генерации «значения аутентификации», основанному на создании восстанавливаемого кода подтверждения подлинности сообщений (MAC). Каждый запрос комментария (RFC 4634) использует хэш SHA256 для генерации MAC. Затем значению хэша присваивается цифровая подпись.

### G.3 Нужно иметь в виду новые проблемы функций хэширования

Функции хэширования – базовые строительные блоки, занимающие центральное место в задаче шифрования, но недавние атаки, рассмотренные Волкером и остальными[56], подорвали наше доверие к классическим конструкциям. В связи с выявленной ненадежностью, проведен ряд новых исследований хэш-функций, в числе первых эти исследования провела компания Intel, подав в НИСТ два независимых и совершенно разных документа, предназначенных для стимуляции международной хэш-конкуренции. Инженеры релейной защиты и управления и инженеры информационной сети должны сотрудничать со специалистами в данной области для совершения прорыва в решении этих проблем.

# Приложение H
# Предотвращение атак переполнения стека

## H.1 Введение

Оливер Мюллер [56] рассуждает о том, что происходит в случае переполнения стека и почему это опасно. Также Мюллер описывает комплексные меры предотвращения атак переполнения стека, возможных для элементов релейной защиты и управления.

Угрозу для элементов релейной защиты и управления представляют переполнения буфера обмена, так как они могут привести к серьезным сбоям функционирования защиты первичного оборудования. Поставщики систем защиты и управления, ответственные за потенциальные уязвимости, реализовали различные способы предотвращения атак переполнения буфера обмена. Инженеры релейной защиты и управления и инженеры информационной сети, не имеющие предварительной подготовки в данной области, должны обращаться за экспертным мнением к независимым консультантам. Их оценка средств релейной защиты и управления должна определить эффективность детекторов, встроенных разработчиками элементов релейной защиты и управления в компиляторы, эти детекторы чувствительны к нарушениям в стеке, спровоцированным с целью использования переполнения стека для получения контроля над системой защиты.

## H.2 Что происходит в случае переполнения стека и почему это опасно

Каждый раз, когда программное приложение системы защиты и управления обращается к подпрограмме командой вызова или через участок цепи, оно сохраняет текущий указатель команд в стек. Оно отмечает его положение перед переходом в новое, поэтому знает, к какому состоянию вернуться после завершения подпрограммы. Такой сохраненный в стеке адрес называется адресом возврата.

Согласно Мюллеру, обычно используемый в системе защиты и управления оборудования высокоуровневый язык программирования помещает локальные переменные подпрограммы на вершину стека (Рисунок H-12). Таким образом, подпрограмма получает собственное место в памяти стека, где она может хранить свои данные. Этот принцип открывает также возможность рекурсивных вызовов, потому что каждый новый вызов подпрограммы получает свой адрес возврата и свои локальные переменные в стеке.

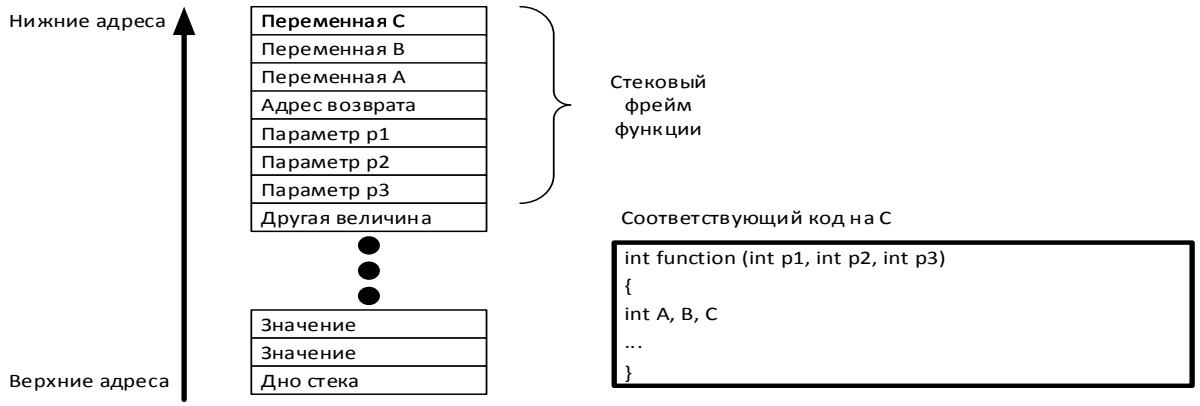



**Рисунок H-12 Строение стека (опубликовано в [57])**

Далее Мюллер объясняет, что из-за наличия возможности заполнения стека таким количеством байтов, которое больше, чем предусмотрено места для конкретной переменной, есть опасность записи в память поверх данных из верхних адресов и, следовательно, ниже конечного расположения переменной в «нижнем адресе» стека (Рисунок H-13). Если копирование процесса не прекращается,

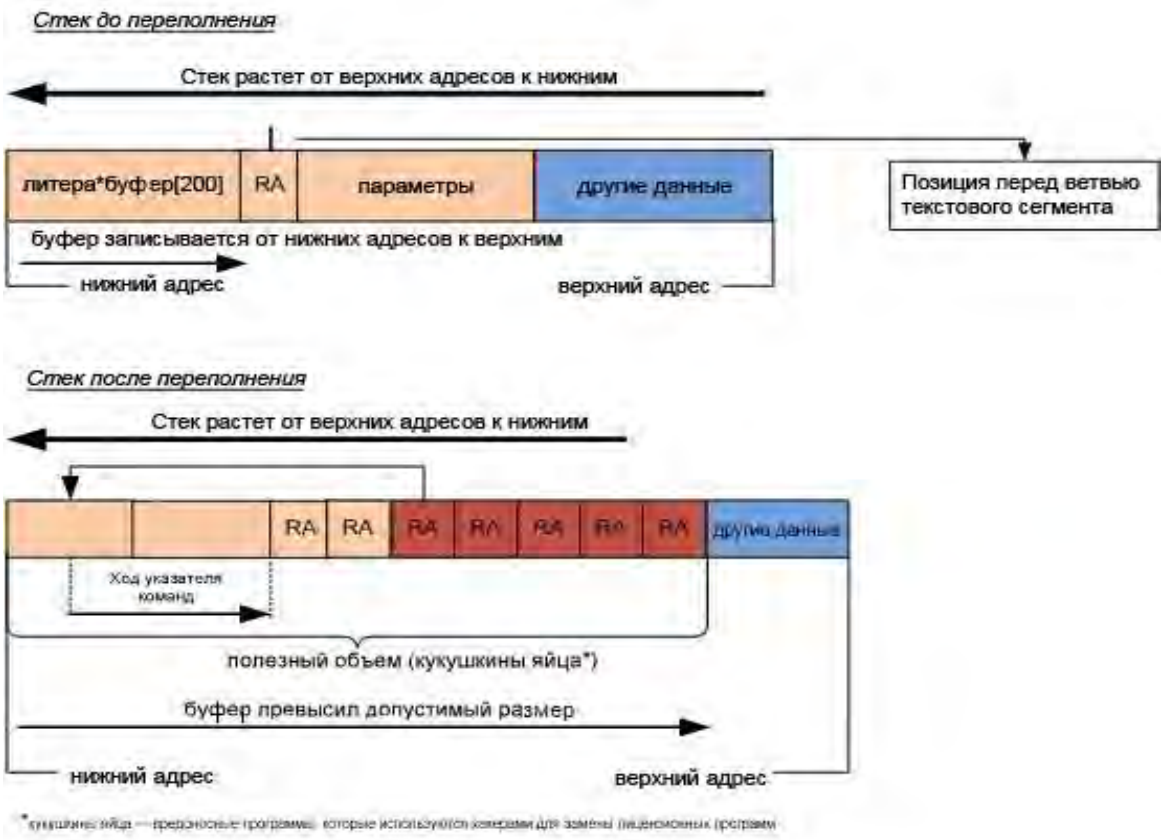



**Рисунок Н-13 Переполнение стека (опубликовано в [57])**

программа в конечном итоге будет перезаписывать адрес возврата, разрушая или генерируя новое значение адреса возврата.
Когда подпрограмма завершена, программа системы защиты и управления считывает адрес возврата, но этот адрес изменился. При обычных обстоятельствах ход программы совершает скачок, представляющий собой обращение программы к непредсказуемому адресу. Весьма велик шанс того, что этот скачок в результате приведет к сегменту, находящемуся за пределами собственной памяти программы, это является сегментным нарушением и приводит к завершению процесса. Вопрос в том, что случается, если цель измененного адреса возврата находится внутри собственной памяти программы. В таком случае, скачок разрешится успешно, а выполнение программы продолжится.

### Н.3 Каким образом нарушитель пользуется схемой

Нарушители пользуются данной схемой, путем переполнения буфера обмена изменяя адрес возврата не на непредсказуемое место, а на определенное. Иными словами, они могут контролировать направление скачка. Мюллер описывает классическую атаку, которая включает так называемый «полезный объем» в избыточных данных, который состоит из трех частей: (1) безоперационный участок (NOP sled), (2) оболочный код (shell code) и (3) новый адрес возврата.

Безоперационный участок состоит из повторяющейся инструкции процессора (NOP), которая не делает ничего, только увеличивает указатель команд – это бездейственный байт-заполнитель. Оболочный код представляет собой короткую программу, написанную нарушителем на языке программирования и соответственно машинным кодом. Обычно он поглощает системные вызовы для получения корневой оболочки. Поэтому такой код и называется «оболочным».

Новый адрес возврата ведет куда-то в безоперационный участок. Если подпрограмма завершает

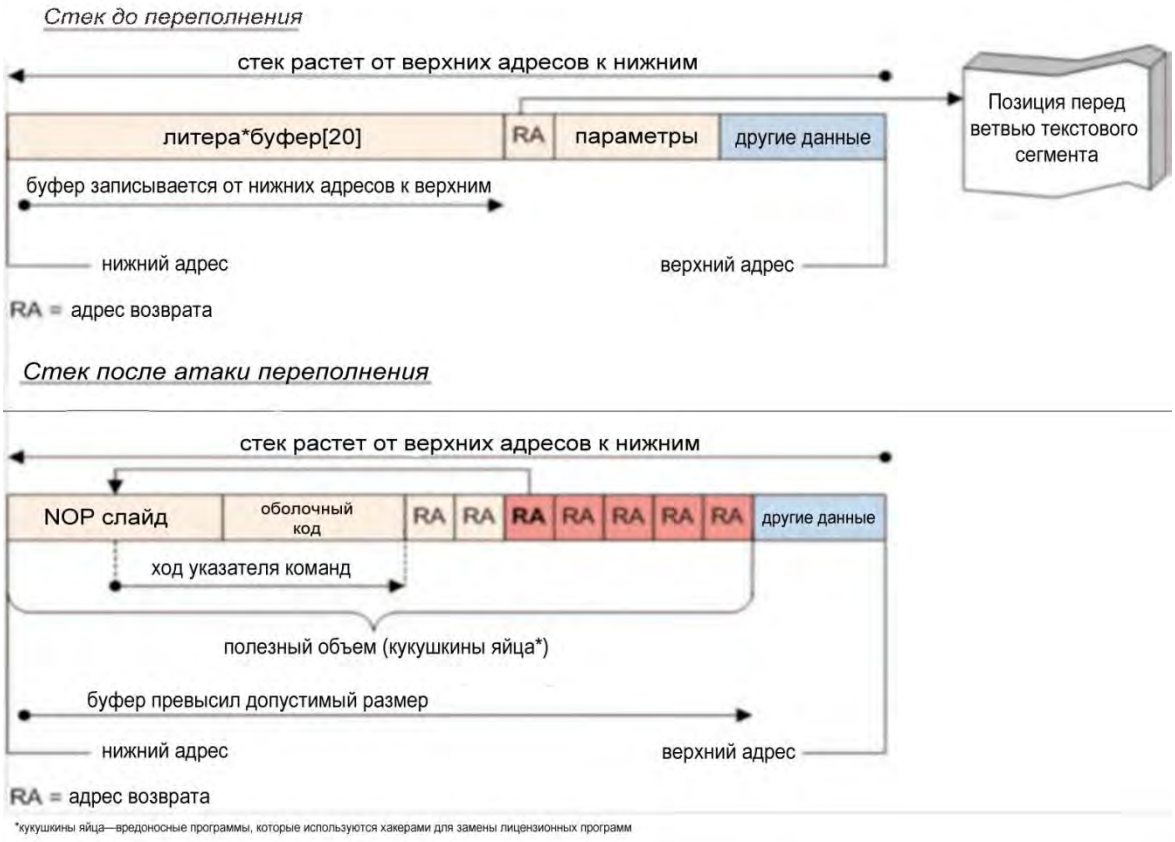



**Рисунок Н-14 Атака переполнения стека (опубликовано в [57])**

программу, будет совершен скачок в безоперационный участок, который начнет выполняться до тех пор, пока программа не достигнет оболочного кода (см. Рисунок Н-14). Оболочный код открывает
корневую оболочку и нарушитель получает контроль над системой.

## Н.4 Хорошая новость – плохая новость

Хорошая новость заключается в том, что атаки с использованием оболочного кода в сегменте стека больше не срабатывают в современных системах защиты и управления. Такие возможности, как невыполняемые стеки, обеспеченные техническими средствами или особенностями операционной системы, предотвращают выполнение внедренного в стек кода. Инженеры релейной защиты и управления и инженеры информационной сети должны выяснять у поставщика оборудования, были ли внедрены невыполняемые стеки; если нет, то чем скомпенсирован этот недостаток. Поставщикам более старых (несовременных) систем защиты и управления необходимо задавать те же вопросы.
К сожалению, существуют и другие приемы, которыми пользуются нарушители. Некоторые из них рассмотрены Мюллером [57], но в любом случае инженеры релейной защиты и управления и инженеры информационной сети должны консультироваться с другими специалистами узкого профиля для решения текущих проблем, связанных с уязвимостями систем защиты и управления перед переполнением стека.

# Приложение I
# Системам защиты и управления необходимо программное обеспечение, гарантирующее масштабируемую защиту на всех уровнях

## I.1 Вступление

Шелдон и Вишик[57] предоставили убедительные доводы в пользу необходимости применения программного обеспечения, гарантирующего масштабируемую защиту на всех уровнях – персональном, частном, общественном и национальном. ОРГ обозначила концепции в области систем защиты и управления, основанные на утверждении, что ненадежное программное обеспечение уже по определению небезопасно. ОРГ выдвинула утверждение, что системы защиты и управления должны быть надежными, но даже надежные системы могут сработать неправильно, если не защищены.

Основываясь на исследованиях проведенных Шелдоном и Вишиком, ОРГ обратила внимание на две идеи:

- «Плавающая точка»: Системы защиты и управления, которые двигаются в разных направлениях, меньше подвержены хакерским атакам и имеют большую отказоустойчивость.

- Диапазон настраиваемой надежности: безопасность настраивается, исходя из определенных, совершаемых системами защиты и управления операций, которые наиболее приоритетны в конкретный момент времени.

Три дополнительные идеи формируют надлежащие концепции обеспечения безопасности систем защиты и управления.

- Надежность*:* многомерные измерения составляют способность систем защиты и управления удовлетворять всем заявленным требованиям для достижения приемлемого уровня доступности целостности системы и её неуязвимости, такой как конфиденциальность данных, гарантирующая в режиме реального времени эффективность, подотчетность, атрибуцию, удобство и простоту использования, а также другие необходимые требования. Точные определения и четко определенные меры, на уровне которых надежность может быть оценена, являются фундаментальным материалом для разработки и эксплуатации надежных систем защиты и управления.

- Масштабируемость*:* способность компонентов систем защиты и управления, сетей и систем расширения функциональности, производительности, сложности и объема удовлетворять необходимым требованиям без потери производительности.

- Сочетаемость*:* создание систем и устройств защиты и управления, удовлетворяющих всем техническим требованиям, из компонентов, подсистем и других систем.

Причина привлекательности данных концепций для инженеров релейной защиты и управления и инженеров информационной сети заключается в возможности их реализации с помощью уже существующих функций обеспечения безопасности на основе существующих программного и аппаратного обеспечения. Эти функции могут быть реализованы в настоящее время или в ближайшем будущем в устройствах с самовосстановлением функций релейной защиты и управления.

## I.2 Идти в ногу со временем

Идти в ногу с развивающимися современными системами защиты и управления – важная задача для систем информационной безопасности. Значительное увеличение производительности систем защиты и управления в сочетании с технологическими достижениями дают потенциал для разработки новых технологий в области информационной безопасности, однако это предоставляет новые возможности злоумышленникам.

Внешние атаки вредоносных программ, таких как Stuxnet, включают в себя преднамеренное проникновение или повреждение систем защиты и управления без информированного согласования с ЭЭС в целом.

Внутренние атаки также представляют собой серьезную угрозу. Они представляют собой вредоносные программы, запущенные из внешних источников, сумевшие проникнуть с помощью различных методов во внутреннюю сеть и потенциально имеющие возможность похитить различные данные. Степень атак варьируется от «низко и медленно», продолжительностью около суток или более, до «быстро и точно» с продолжительностью от миллисекунды или даже быстрее. Нормальная динамическая кибер-наведенная активность работы системы защиты и управления с легкостью помешает обнаружению.

Главной проблемой обеспечения безопасности является непрерывное развитие средств информационных атак. Защита от известных угроз не подходит для новых видов атак. Традиционные методологии управления рисками обеспечивают только общие принципы и советы по оценке информационной безопасности, но не имеют конкретных руководящих принципов для оценки возникающих угроз. Новые подходы к обеспечению информационной безопасности являются предметом продолжающихся исследований и дискуссий, в которых инженеры релейной защиты и управления и инженеры информационной сети должны принимать активное участие.

### I.3 Диапазон настраиваемой надежности

Диапазон настраиваемой надежности поддерживает контекстно-зависимые решения релейной защиты. ОРГ пришла к выводу, что операции систем защиты и управления уникальны и общие принципы построения информационной безопасности к системам защиты и управления неприменимы. Действительно, эксплуатационные ограничения требуют различных или, лучше сказать, индивидуальных решений для систем защиты и управления. Защите необходимо разрешить принимать обоснованные целевые решения для обеспечения инженеров релейной защиты и управления и инженеров информационной сети набором контекстно-целевых функций реализации согласованной политики на основе комплексного набора вариантов информационной безопасности или функций по умолчанию, подходящих для своих задач и обязанностей. Все это включает в себя правила и свойства, используемые инженерами, которые занимаются разработкой и обеспечением подходов идентификации и аутентификации, правил информационных потоков, устойчивости распределения постоянно работающих механизмов, уровней оперативного мониторинга и адаптации к ним.

Диапазон настраиваемой надежности предполагает наличие такой инфраструктуры, части которой объединены для поддержки различных целевых сред, максимально используя управление идентификационной информацией и метод компоновки для достижения надежного согласования функций и надежного управления.

### I.4 Метод «плавающей точки» для обеспечения устойчивости посредством «увеличенной скорости»

Целью метода «плавающей точки» является уменьшение возможностей для взлома при одновременном улучшении функций самовосстановления и отказоустойчивости систем защиты и управления. Метод «плавающей точки» должен сохранять работоспособность, даже если полная безопасность недостижима, т. к. системы защиты и управления должны быть в состоянии продолжать безопасные и надежные операции, даже будучи подверженными кибератаке.

Алгоритм «плавающей точки» должен сбить с толку злоумышленников, а не инженеров, обслуживающих ЭЭС в целом, которым из-за специфических трудностей требуются дополнительные возможности управления для поддержания системы со всей присущей ей сложностью. Целесообразность применения этих возможностей требует тщательного анализа затрат и выгод, а также разработки новых показателей для обеспечения их надлежащего применения. Кроме того, инновационные механизмы поддержки принятия решений, осуществляемые совместно инженерами релейной защиты и управления и инженерами информационной сети, легли в основу их успешного применения. ОРГ приводит следующие

рекомендации:

• Механизмы «плавающей точки» должны быстро адаптироваться для сокращения возможностей по взлому систем защиты и управления, а также сокращения возможности каскадной потери передачи в ЭЭС.

• Механизмы «плавающей точки» должны в режиме реального времени обеспечивать распознавание угроз и противодействие им.

• Механизмы «плавающей точки» должны учитывать специальное распределение ключей, наряду с быстрым и устойчивым механизмом смены ключа, который требует сложной логики принятия решений, в том числе расширенных возможностей для обеспечения ситуационной осведомленности, поддающихся проверке показателей для поддержки автоматической обработки данных, принятия решений практически в режиме реального времени, масштабируемых методов с высоким уровнем контроля и моделей для их проверки.

# Приложение J
# Участие инженеров релейной защиты и управления в аудите конфигурации

## J.1 Необходимость аудита конфигурации систем защиты и управления

Аудит конфигурации – это процесс проверки конфигурации объектов систем защиты и управления с целью обеспечения их совпадения с заявленными протоколами безопасности. Инженеры релейной защиты и управления и инженеры информационной сети должны принимать активное участие в осуществлении аудита конфигурации, т. к. именно они знают о потенциальных последствиях в случае неправильно настроенной системы защиты и управления.

Аудит конфигурации систем защиты и управления служит не только для проверки, но и обеспечивает три основных преимущества:

**Повышает безопасность с использованием актуальной информации**, поскольку инженеры релейной защиты и управления имеют возможность быстро и эффективно обеспечить правильную и безопасную основу для конфигурации объектов и следить за ее постепенными изменениями.

**Снижает нагрузку и повышает эффективность операций** защиты с улучшенным анализом обстановки, в том числе изменения и появление новых (плановых и внеплановых) значимых и осуществимых задач.

При совместной работе инженеров релейной защиты и управления и инженеров информационной сети главной задачей при аудите является проверка конфигурации всех компонентов релейной защиты и управления в среде подстанции, чтобы убедиться, что они имеют правильные настройки. Это включает в себя аудит новых компонентов системы защиты и управления и мониторинг изменений для проверки правильности установки. В связи с важностью конфигурации систем защиты и управления в области защиты конфиденциальной информации появляется все больше и больше стандартов, таких как МЭК 62351 и МЭК 62443, и нормативных актов, таких как NERC CIP, которые предусматривают необходимость регулярного и последовательного аудита конфигураций систем защиты и управления.

## J.2 Важность автоматизации

Проверка конфигурации систем защиты и управления, проведенная вручную, требует огромных затрат времени и сил, что может негативно сказаться на работе систем защиты и управления. Каждый компонент системы защиты и управления имеет тысячи вариантов конфигурации, которым необходим аудит, например, длина и сложность пароля, уровень доступа к файлам, целостность файлов и установленное программное обеспечение. Кроме того, без автоматического обнаружения новые компоненты и изменения могут быть не идентифицированы или просто проигнорированы.

Автоматические механизмы обнаружения в сочетании с семантикой четко определенных данных, несомненно, являются решением. Реализация МЭК 61850 является отличным способом обеспечения необходимой автоматизации для поддержки аудита конфигурации системы защиты и управления.

### J.2.1 Мониторинг изменения конфигурации

Важной задачей инженеров релейной защиты и управления и инженеров информационной сети является обеспечение такой конфигурации системы, которая оставалась бы совместимой с внутренней и регуляторной политикой безопасности. Цена ошибки в настройках конфигурации или случайного пропуска компонента системы защиты может быть катастрофичной. Для этого достаточно всего лишь неправильно настроить релейную защиту или случайно оставить порт обслуживания открытым. В такой ситуации складывается благоприятная обстановка для хакерских

атак.

### A.2.2 Основы аудита конфигурации

Назначение аудита конфигурации: собрать информацию о компонентах системы защиты и управления в сети подстанции и сравнить эти конфигурации с нужным состоянием.

Соответствие является ключевым фактором для инженеров релейной защиты и управления и инженеров информационной сети, поддерживающего аудит конфигурации. Однако проблема состоит в том, что соответствие не всегда достигается. Аналогично этому, некоторые системы защиты и управления способны продемонстрировать соответствие без обеспечения безопасности. Ключ к успеху заключается в использовании решения для аудита конфигурации, которое оптимизирует доступный бюджет для повышения безопасности и обеспечения соответствия.

## J.3 Аудит против управления

Целью аудита является обеспечение рекомендуемой и требуемой конфигурации системы защиты и управления подстанции.

Тот же инструмент, который используется инженерами релейной защиты и управления и инженерами информационной сети для внесения санкционированных изменений, может предоставить возможность злоумышленнику произвести незаконные изменения. Кроме того, когда решение по управлению не отвечает требованиям оригинального ПО, нового или специального компонента системы защиты и управления, то это решение не распознается и игнорируется.

Суть заключается в том, что инструменты управления конфигурацией, которые обеспечивают системы поддержки, не являются инструментом для аудита системы защиты и управления. Лучше всего использовать специализированные инструменты для аудита. Вот несколько примеров, подтверждающих данную необходимость.

### J.3.1 Контроль целостности

Одним из основных понятий аудита конфигурации системы защиты и управления является мониторинг целостности файлов. Концепция проста: создать список важных системных файлов защиты и управления и регулярно проверять файлы на предмет изменений. Часто используемый в качестве сигнала сортировки, контроль целостности файлов полезен для предупредительного аудита и служб безопасности, когда меняются высокостабильные файлы системы защиты и управления, которые обычно были неизменными.

Установим частоту мониторинга целостности файлов в протоколе безопасности для работы системы защиты и управления.

### J.3.2 С агентом или без агента

Когда проводится аудит или сохранение конфигурации компонентов системы защиты и управления, для прежней версии ПО устанавливается часть программного обеспечения, которое называется агент целевой машины. Недостатком использования агента является требовательность к ресурсам памяти и процессоров в дополнение к необходимости наличия канала связи с центральной консолью управления. Для системы защиты и управления подстанции это неприемлемое решение, поэтому лучше не использовать агентов.

Метод без агентов не требует установки на целевой машине. Устранение необходимости "контакта" с каждым компонентом системы защиты и управления для проведения аудита обеспечивает ряд преимуществ:

- метод значительно быстрее реализуется
- меньшие затраты на покупку и эксплуатацию
- меньшее использование системных ресурсов, чем при методе с использованием агента
- возможность охвата большего количества компонентов системы защиты и управления.

•обеспечивает охват устройств, которые не могут поддерживать, и агентов.

Метод без агентов не ссылается на ранее определенный список компонентов системы защиты и управления. Вместо этого, они способны обнаружить и проверить весь набор компонентов системы защиты и управления, установленных на подстанции, некоторые из которых могут быть заранее неизвестны.

### A.3.3 Оперативная информация

Как и вопрос получения ключевой информации, существует еще один важный вопрос для инженеров релейной защиты и управления и инженеров информационной сети: «Что можно сделать с полученной информацией?».

Оперативная информация требует расстановки приоритетов компонентов системы защиты и управления в сочетании с показателями, которые производят правильный отчет для целевых получателей информации. Существенной особенностью является возможность определить приоритеты информации на основе различных критериев для удовлетворения запросов различных получателей информации, включая специалиста по безопасности, менеджеров по эксплуатации и руководящий персонал.

Внедряйте эффективные решения для обеспечения полезной информацией, подкрепленной опытными данными. Отчеты являются комплексными, гибкими и обеспечивают возможность сосредоточиться на конкретном получателе информации, представляя информацию (не сырые данные), чтобы принимать более обоснованные решения.

# Приложение K
# Своевременное выявление возможных угроз

## K.1 Сокращение времени отклика защиты требует своевременного распознавания угрозы

Системы защиты защищают основное оборудование в автоматическом режиме. Одним из подходов к сокращению времени отклика защиты является использование "частотного анализа паттернов" в рамках интеллектуального анализа данных. Частотные паттерны определяют последовательности и подмножества, которые входят в набор данных с определенным уровнем частоты. Последовательным анализом паттернов является обнаружение частых элементов подпоследовательностей. И частотные, и последовательные виды анализа полезны при корреляции информации о направлении атаки с использованием частот и последовательностей. Обычно, паттерн алгоритма обнаружения коррелирует данные. Симмонс [58] расширяет этот подход к системе идентификации уязвимостей (СИУ), где уязвимости связаны с конкретными настройками приложения. Данная техническая брошюра рассматривает применение СИУ для настройки системы защиты и управления.

Точная индексация данных, классификация и кластеризация предоставляет исходные данные, необходимые для определения потенциальных последствий предполагаемой кибер-атаки на систему защиты и управления, например, данные, собранные и зарегистрированные с помощью защитных реле, датчиков и контроллеров присоединений для нахождения возможных направлений кибератак на систему защиты и управления. Обработка файлов регистрации и настроек баз данных позволяет проанализировать текущее состояние оборудования. Также производится запрос информации, хранящейся в сервере архивных данных, чтобы получить частотные и последовательные элементы данных.

Таким образом, наиболее важные данные системы защиты и управления становятся доступными. Когда они доступны, новые алгоритмы и высокоскоростная обработка событий после операции определят и широкий спектр действий, которые может совершить злоумышленник, чтобы обойти протоколы классификации и отклика.

## K.2 Структура системы разрешения проблем безопасности

Симмонс [37] предложил перспективную систему разрешения проблем безопасности (СПРБ), которая легко приспосабливается к извлечению и распространению информации о векторе атаки на систему защиты и управления. Идея СПРБ заключается в использовании алгоритма классификации, который состоит из двух основных методов: метод классификации и метод дерева решений. Метод классификации идентифицирует соответствующий вектор атаки для классификации. После классификации, СПРБ представляет информацию для анализа.

На рисунке K-15 показана возможная схема с учетом особенностей систем защиты и управления для определения и классификации реакций на инициированные кибератаки. Цель состоит в том, чтобы максимально использовать имеющиеся ИЭУ релейной защиты и серверы данных системы защиты и управления.

## K.3 Онтологии, используемые для организации данных, используемых для обработки инициированной кибератаки

Онтология[21] представляет собой точно определенные концепции, относящиеся к конкретной области системы защиты и связям между этими концепциями для создания организованной базы данных направлений кибератак. Онтология использует входные данные из базы данных предпринятых кибератак и алгоритм классификации для поддержки идентификации, реагирования и противодействия предпринятым кибератакам. Правильно разработанный процессор онтологии будет фиксировать детали атаки из базы данных, чтобы начать анализ атаки. Для процессора

[21] Онтология - распространенный способ систематизации знаний и включения описаний объектов и связей.

онтологий необходимо установить следующие соотношения:

**связан с**: субъектом (человеком или ИЭУ), назначающим действие задачи
**есть в наличии**: информация, необходимая для выполнения действия
**является**: вариантом, связанным с конкретизацией абстрактного класса объекта; например, резервная защита является конкретизацией класса устройств релейной защиты
**состоит из**: совокупности атрибутов, описывающих данные объект
**утвержден**: субъектом (человеком, ИЭУ, механизмом аутентификации), который разрешает выполнение задачи
**влияние следующих факторов**: это связь, описывающая собственное влияние действия

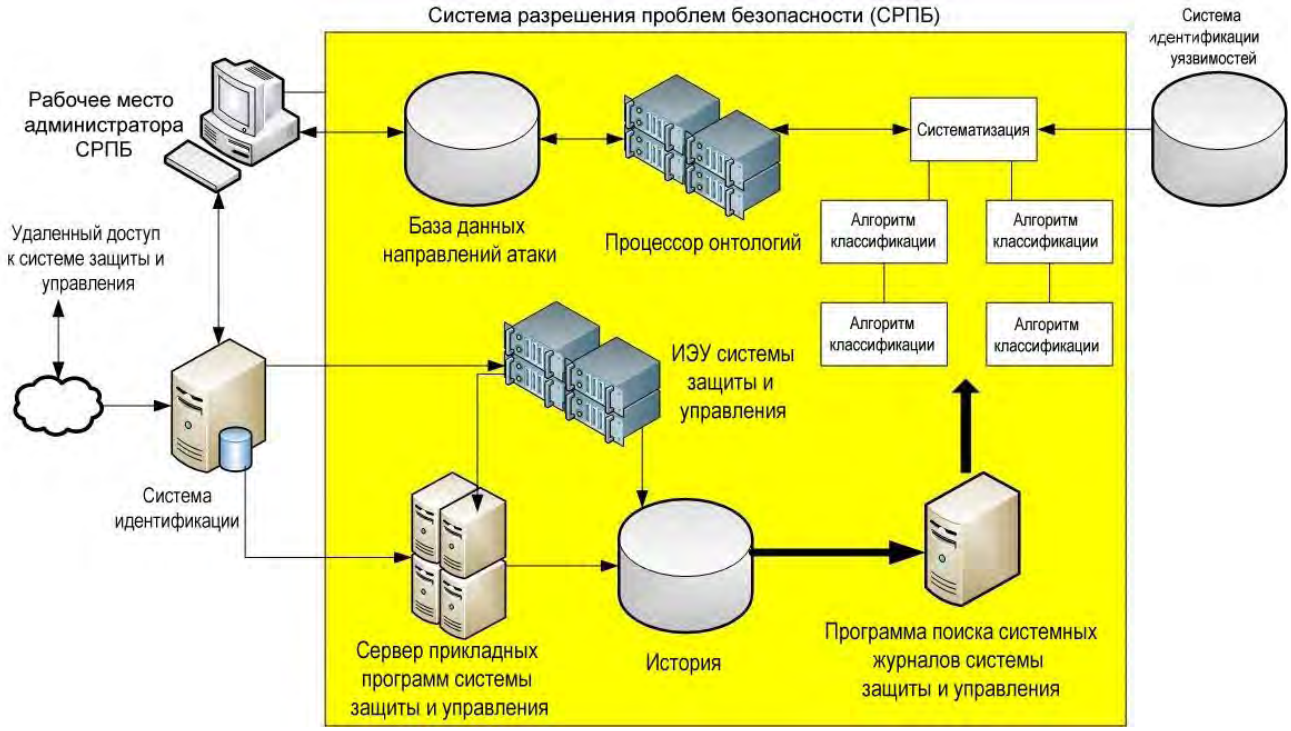



**Рисунок К-15: Возможная схема системы разрешения проблем безопасности.**

## К.4 Систематизация кибератак на основе последствий

Предложенный алгоритм классификации использует частотный и последовательный анализ паттернов для классификации информации о направлении кибератаки. Затем эта информация хранится в базе данных предпринятых кибератак для выявления сопутствовавших атак и перспективных защит.

### К.4.1 Взаимодействие с угрозой

Когда совершается атака на систему защиты и управления, существует вероятность того, что она имеет несколько направлений. Направление атаки определяется как путь, с помощью которого злоумышленник может получить доступ к системе защиты и управления, как правило, через точки доступа локальной сети подстанции, например, через сетевой интерфейс. Из-за присущей системам защиты и управления устойчивости, при распознавании угроз выявляются также уязвимости системы защиты и управления, так как для успешной атаки могут потребоваться всего лишь несколько слабых мест системы.

Используя язык моделирования, ОРГ разработала схему, изображенную на рисунке К-16, которая показывает классово-объектные отношения, описывающие взаимодействие, необходимое для устранения предпринятой кибератаки на систему защиты и управления. Свойствами угрозы являются: её тип, цель, место и вероятность успешной атаки. Если удается их обнаружить, то

перечисляемые угрозы являются «частью» угрозы с кардинальностью 0, что означает, что может не быть пронумерованных угроз (0), а может быть много пронумерованных угроз (*).

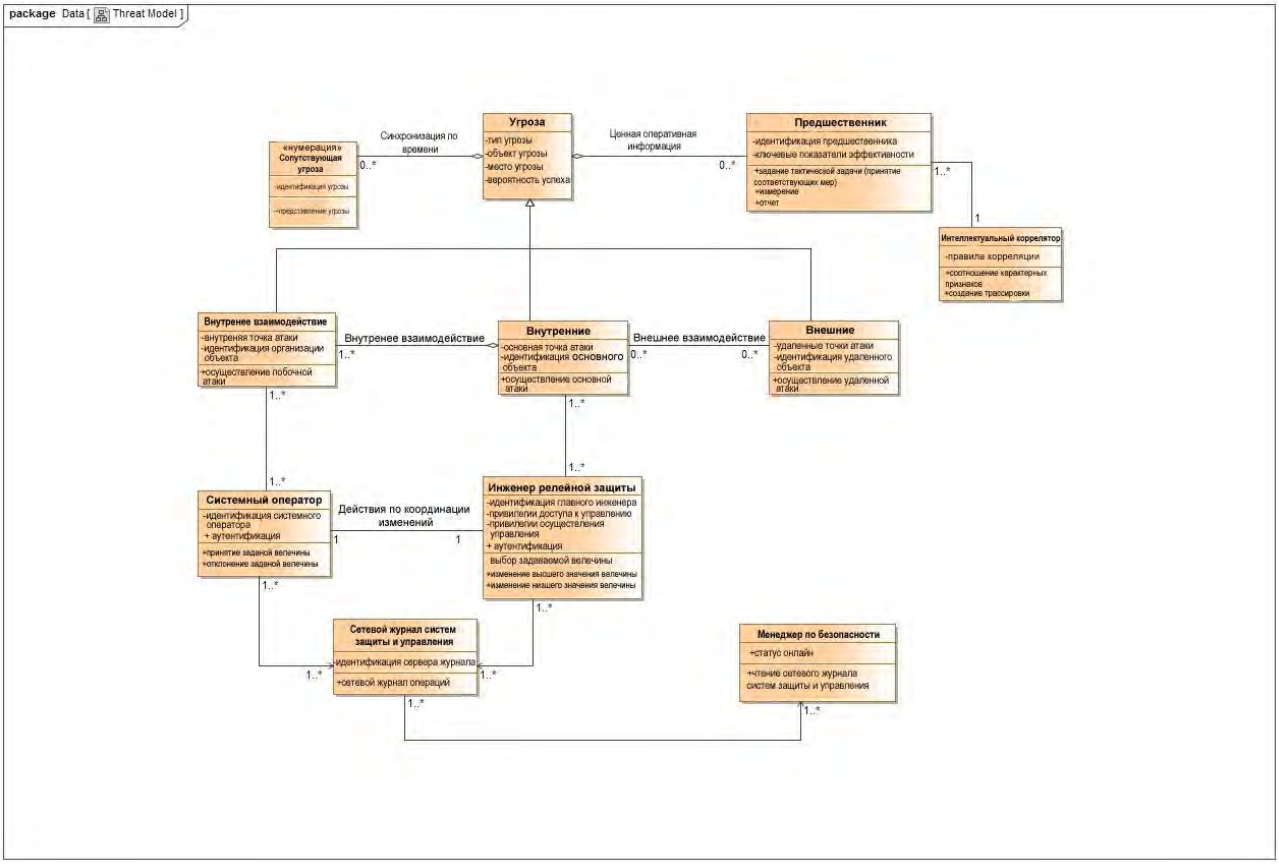



**Рисунок К-16: Взаимодействие с угрозами**

Точно так же, если можно их найти, предшественники используют реализуемые сведения для того, чтобы идентифицировать и классифицировать угрозы.

Классификация как внутренних, так и внешних угроз называется специализацией класса угрозы. Опять же, если можно распознать предшествующие паттерны, устанавливается взаимодействие внутренних и внешних угроз. То же самое верно и для внутреннего сотрудничества между организациями в рамках ЭЭСОП, за исключением случая, когда есть хотя бы один случай внутренней связи.

### К.4.2 Цели и возможности защиты.

Контролер присоединения или АРМ (автоматизированное рабочее место) может представлять интерес для злоумышленника, т. к. успешная атака может привести к серьезным последствиям для подстанции. Например, АРМ может быть в состоянии контролировать всю подстанцию, где контролер присоединения может управлять номинальной мощностью оборудования.

Как правило, АРМ и контроллеры присоединения связаны между собой и с конкретными ИЭУ с помощью локальной сети. Поэтому существуют некоторые проблемы безопасности для данной схемы.

- Большинство устаревших и некоторые современные контроллеры присоединений взаимодействуют в текстовом формате и не имеют функций безопасности, например, таких как аутентификация.

- Инженеры релейной защиты и управления редко принимают во внимание вопрос информационной безопасности при настройке АРМ и контролеров присоединения.

•В последнее время воздушный зазор, на который полагались инженеры релейной защиты и управления на протяжении многих лет находится на стадии исчезновения – современные подстанции подсоединены к разным системам, исходя из коммерческих соображений.

•Обновление АРМ и контроллеров присоединений на подстанциях происходит редко, потому что в процессе технического обслуживания нарушается нормальная работа этих систем и ввиду трудоёмкости процесса.

При такой перспективе кибератаки смогут принимать самые разные формы. В соответствии с тем ограничением, что коррекция параметров всех контроллеров присоединений и АРМ является непрактичной, инженеры-релейщики должны найти контрмеры для защиты данного оборудования от наиболее вероятных угроз. В первую очередь надо установить электронные периметры безопасности (ESPs), чтобы увеличить физические периметры безопасности (PSPs).

Надежный электронный периметр безопасности должен, как минимум, использовать:

• Перечень всех точек доступа к ESP,

• Электронный периметр безопасности должен находиться в пределах физических периметров безопасности,

• Контроль доступа по сообщениям, по умолчанию отказывающий всем в доступе и требующий, чтобы было указано явное разрешение,

• Порты и сканирование уязвимостей на каждой точке доступа, необходимые для того, чтобы убедиться, что открыты только самые необходимые порты,

• Связь между ИЭУ должна быть зашифрована,

• Процесс управления изменениями для каждой точки доступа, который должен быть в рабочем состоянии

• Контроль ненормальных действий и своевременный отчет от всех точек доступа с техническим контролем.

Надежный физический периметр безопасности должен, как минимум, использовать:

• Перечень всех точек доступа к физическому периметру безопасности,

• Периодический обзор, переаттестацию и обновление всех своих прав доступа,

• Установки контроля доступа, такие как ключ-карты, смарт-карты в соответствии с правилами разграничения доступа физического периметра безопасности, и

• Установленную сигнализацию обнаружения несанкционированного входа.

При контроле с помощью ЕПБ и ФПБ злоумышленнику потребуется взломать одного или несколько штатных сотрудников, чтобы получить доступ или найти брешь либо в ЕПБ, либо в ФПБ. может получить доступ или найти уязвимость в любом из периметров безопасности только, если ему будет помогать кто-то из обслуживающего персонала. Такое несанкционированное разглашение информации предоставит необходимые знания и очень высокий уровень доступа для того, чтобы успешно инициировать кибератаку.

И, наконец, АРМ и контроллеры присоединений, работающие на базе ПК ( например, использующие Windows XP) должны иметь встроенные средства управления безопасностью для защиты от вредоносных программ, которые могут быть введены с помощью других средств. Для получения дополнительной информации по этой теме см. пункт 6.4.

# Приложение L
# Модель оценки CySeMoL

## L.1 Введение в CySeMoL

Язык моделирования для информационной безопасности (CySeMoL) – это язык моделирования и программное средство, которые могут быть использованы для анализа уровня информационной безопасности на предприятиях [37].

Основная цель CySeMoL - дать возможность пользователям создавать модели архитектуры систем и производить расчеты вероятности успеха различных кибератак. Поскольку модель содержит информацию о том, как параметры модели объекта зависят друг от друга, от пользователя CySeMoL не требуется специальных знаний. Для проведения расчетов пользователям необходимо лишь построить модель архитектуры системы (напр. сервисов, операционных систем, сетей и пользователей) и указать параметры (напр. используется ли криптография, установлены ли обновления).

Классы CySeMoL содержат такие компоненты информационной техники, как *операционная система* (напр. Windows XP) и *система сетевой защиты*, процессы, такие как *программа уведомления о мерах безопасности* и *субъекты*, которыми являются пользователи. Каждый объект содержит набор параметров, которые могут негативно повлиять на сам объект или на контрмеры, связанные с ним. Эти параметры связаны друг с другом различными путями. Например, пароли или *учетная запись* могут быть получены путем обмана пользователей, но вероятность успеха такой атаки зависит от того, состоит ли *субъект*, владеющий *учетной записью*, в программе уведомления о *мерах безопасности*. Каждый параметр в CySeMoL может иметь значения «истина» или «ложь» и представляет либо вероятность успеха атаки, либо вероятность эффективного противодействия.

Всего CySeMoL содержит 22 объекта, 102 параметра и 32 связи. На рисунке L-17 показано общее описание объектов языка моделирования и их связи. На рисунке L-17, в верхнем сегменте прямоугольника, представляющего объект, описаны контрмеры, связанные с классом данного объекта. В нижнем сегменте описаны операции атаки, выполненные в отношении класса объекта. Штриховой линией представлены связи между объектами. Например, *субъект* может быть владельцем *учетной записи* и быть частью программы уведомления о мерах безопасности.

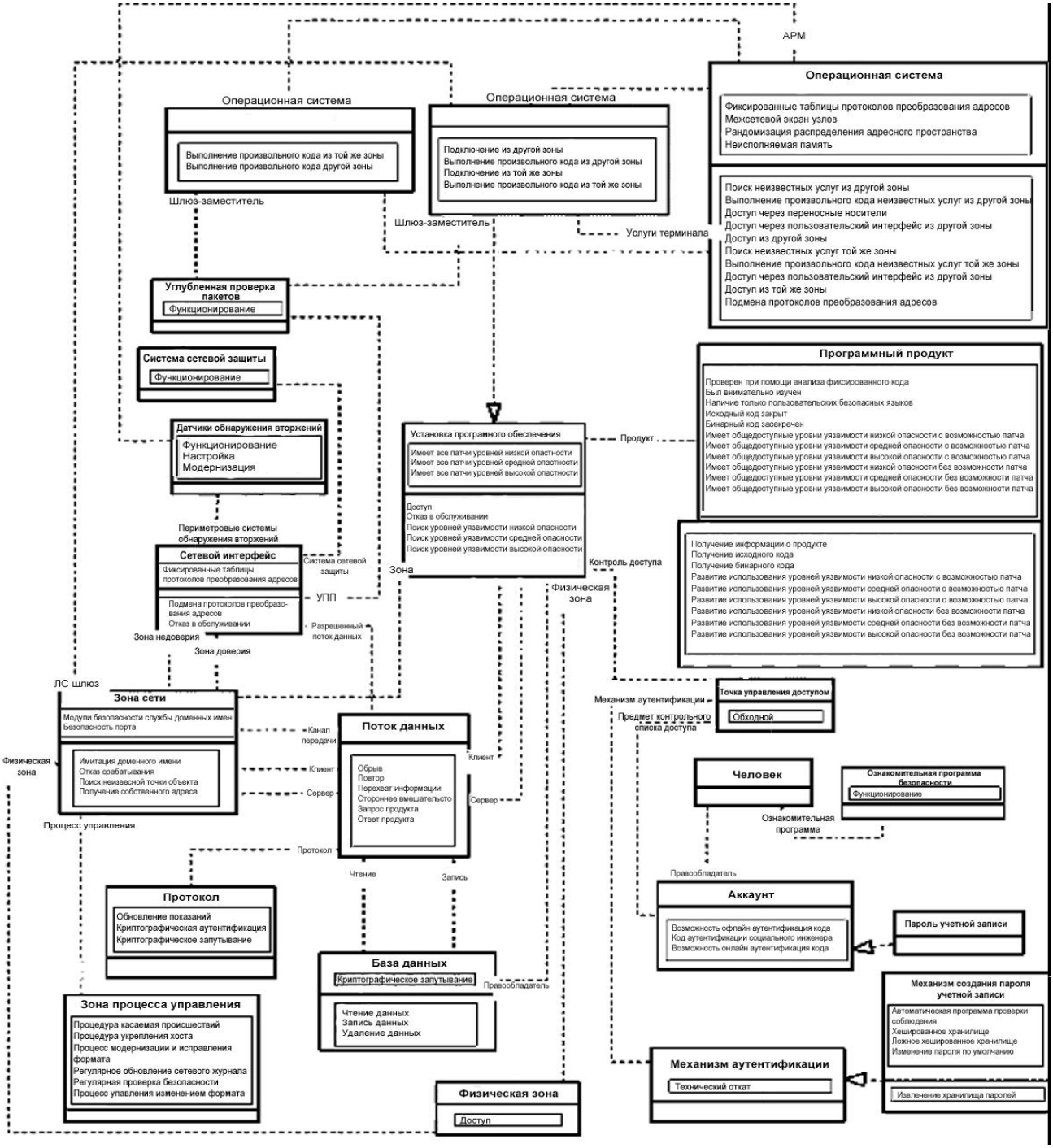



**Рисунок L-17 Общее описание объектов CySeMoL и их связи**

Операции атаки и соответствующие контрмеры в CySeMoL могут быть условно разбиты на семь категорий (Табл. L-11). С помощью публикаций и обсуждения со специалистами в данной области, были определены характерные признаки каждой из них. Вероятность успеха атаки зависит от условий ее проведения и контрмер, направленных на ее подавление. Подход состоит в том, чтобы за основу подсчета вероятности взять допущение, что злоумышленник – профессионал в области проникновения в систему, имеющий в запасе одну неделю на проведение атаки. Например, вероятность того, что взломщик обнаружит новую уязвимость (так называемую «уязвимость нулевого дня») в программном обеспечении в течение одной недели зависит от нескольких факторов[59]:

- Способен ли злоумышленник идентифицировать программное обеспечение

- Удалось ли злоумышленнику заполучить бинарный или исходный код
- Способен ли злоумышленник определить, что программное обеспечение тщательно проверяется другими лицами
- Способен ли злоумышленник определить, что программное обеспечение было разработано на языке, «защищенном» от переполнения буфера (напр. Java в сравнении с C++)
- Способен ли злоумышленник определить, было ли программное обеспечение протестировано на предмет безопасности с помощью утилит статического анализа кода.

**Таблица L-11 Краткое описание категорий CySeMoL**

| Категория CySeMoL | Качественное подтверждение | Количественные показатели |
|---|---|---|
| Обнаружение новых уязвимостей | Публикации и 3 эксперта. | Классический метод Кука, применённый к суждениям 17 специалистов. |
| Удалённая атака на основе использования произвольного кода | Публикации, пробное исследование и 3 эксперта. | Классический метод Кука, примененный к суждениям 21 специалиста. |
| Обнаружение проникновения | Публикации и 3 эксперта. | Классический метод Кука, примененный к суждениям 165 специалистов. |
| Атаки отказов в обслуживании (ОО) | Публикации и 2 эксперта. | Классический метод Кука, примененный к суждениям 23 специалистов. |
| Использование ошибок в конфигурации сети | Публикации и 2 специалиста в данной области. | Данные публикаций и суждения 4 специалистов. |
| Атаки на парольную защиту | Публикации и специалист в данной области. | Обзор и обобщение данных о подборах паролей и возможностях радужных таблиц. |
| Метод проникновения на основе социальной психологии (социальный инжиниринг) | Публикации. | Эксперименты в сфере атак на основе социального инжиниринга. |

Для проведения анализа необходимо обратиться ко всем возможным комбинациям определяющих параметров в CySeMoL.

- Существует $2^6$ различных комбинаций, дающих 64 вероятные комбинации, которые позволяют найти новую уязвимость, обладающую 6 влияющими параметрами.
- Допустить, что другие лица тщательно следят за программным обеспечением, но оно не было разработано с помощью языков, «защищенных» от переполнения буфера.
- Допустить, что безопасность программного обеспечения протестирована с помощью утилит статического анализа кода.
- Если взломщик может идентифицировать программное обеспечение и заполучить двоичный код, но не исходный, тогда существует 20%-я вероятность нахождения «уязвимости нулевого дня» в течение недели [9].
- Однако, если доступен исходный код, вероятность повышается до 73% [9].

Большинство (82%) оценок вероятности в CySeMoL детерминированные, т.е., либо известно, что атака возможна, либо известно, что не возможна. К примеру, злоумышленнику практически невозможно обнаружить «уязвимость нулевого дня», если он не имеет возможности идентифицировать программное обеспечение, получить его копию или проект.

Если возможно, система выдает недетерминированные подсчеты на основе эмпирических исследований. К сожалению, надежные результаты подобного рода доступны не для всех типов атак, рассматриваемых в CySeMoL. Для осуществления количественного анализа многие оценки основываются на исходных данных, собранных специалистами. Так как ценность суждений специалистов различается, для подсчета реального веса каждого из них используется классический метод Кука[9]. По существу, метод Кука предполагает тест на знания –экспертам задаются вопросы, ответы на которые известны на момент анализа. Суждения специалиста, точно и уверенно ответившего на вопросы, считаются более весомыми, нежели специалиста, отвечавшего неточно и неуверенно.

Для того, чтобы сделать моделирование и подсчеты удобными для пользования, CySeMoL реализован в виде программного средства. Также оно способно автоматически создавать модели CySeMoL на основе результатов, получаемых от автоматизированных сканеров, предназначенных для поиска уязвимостей, таких как Nessus[60].

## L.2 Модели сети

### L.2.1 Описание графического представления

Для лучшего понимания рисунков, приведенных в пункте L.2, читателю предлагается ознакомиться с [61]. На рисунках отражены реальные сети в системах защиты и управления в представлении, привычном для инженеров.

### L.2.2 Описание модели сети

Рисунок L-18 представляет собой общую топологическую схему сети. В пределах подстанции, локальная сеть (ЛС) отделена от интернета внутренней сетью организации. Каждая из них защищена хорошо настроенными сетевыми экранами. В данной технической брошюре анализ производится исходя из предположения, что злоумышленник не имеет возможности заполучить физический доступ к компонентам какой-либо части сети. Персонал, имеющий доступ к внутренней сети организации, имеет доступ к *шлюзу удаленного доступа,* который служит для предоставления доступа к ЛС системы защиты и управления уполномоченному персоналу.

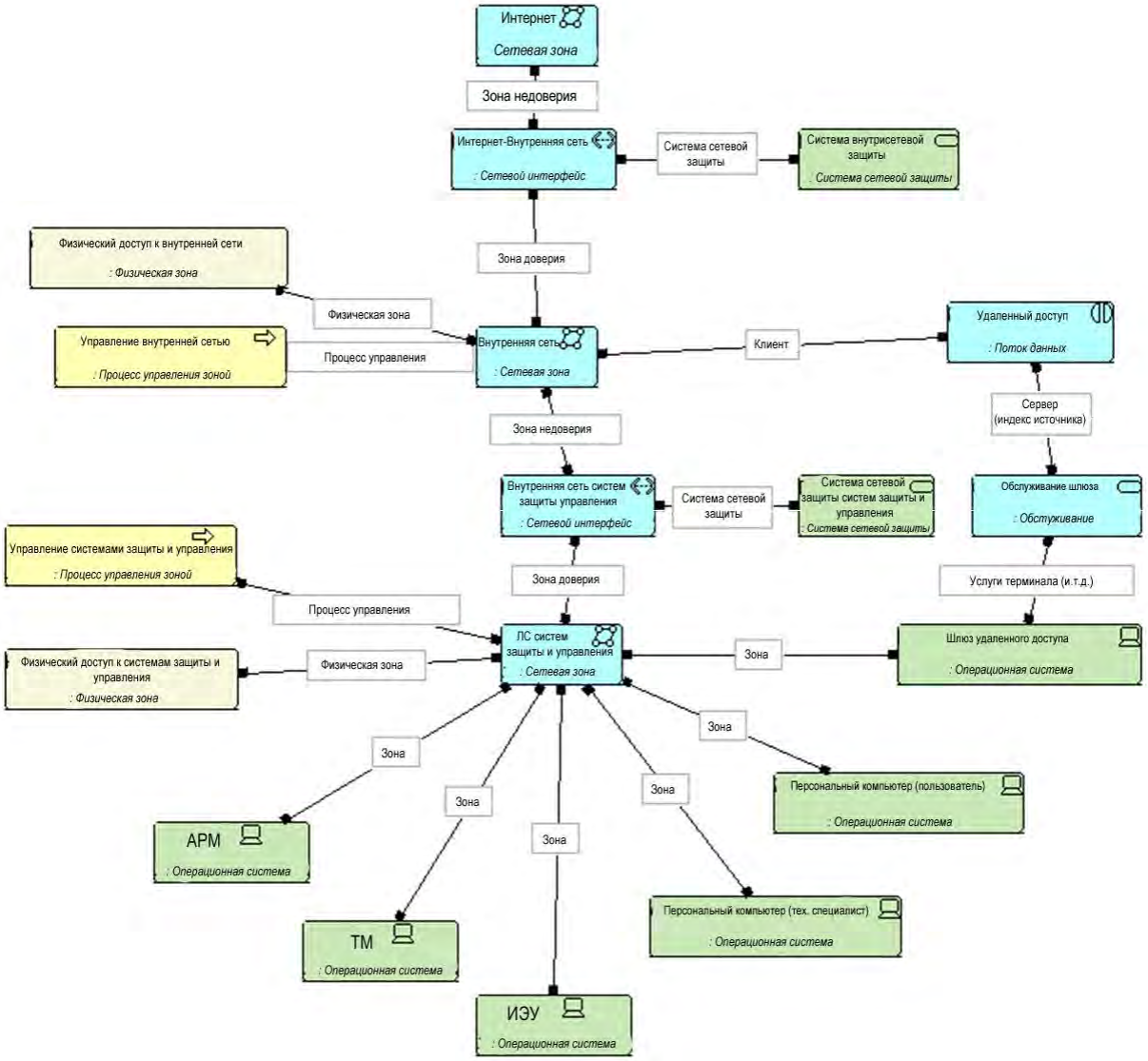



**Рисунок L-18 Общая схема модели сети**

### L.2.3 Краткое описание удаленного доступа к оборудованию системы защиты и управления из внутренней сети

На рисунке L-19 показаны компоненты, которые принимают участие в процессе предоставления удаленного доступа к ЛС системы защиты и управления. Персонал, имеющий доступ к внутренней сети компании, обладающий соответствующими учетными данными, также может получить доступ к ИЭУ (терминалам системы защиты и управления), автоматизированному рабочему месту (АРМ) и к устройствам телемеханики. АРМ и устройства телемеханики (ТМ) используют зашифрованные протоколы (Протокол удаленного рабочего стола, RDP, и протокол «безопасной оболочки», SSH). Для доступа к ИЭУ (терминалам системы защиты и управления) используется незашифрованный протокол Telnet.

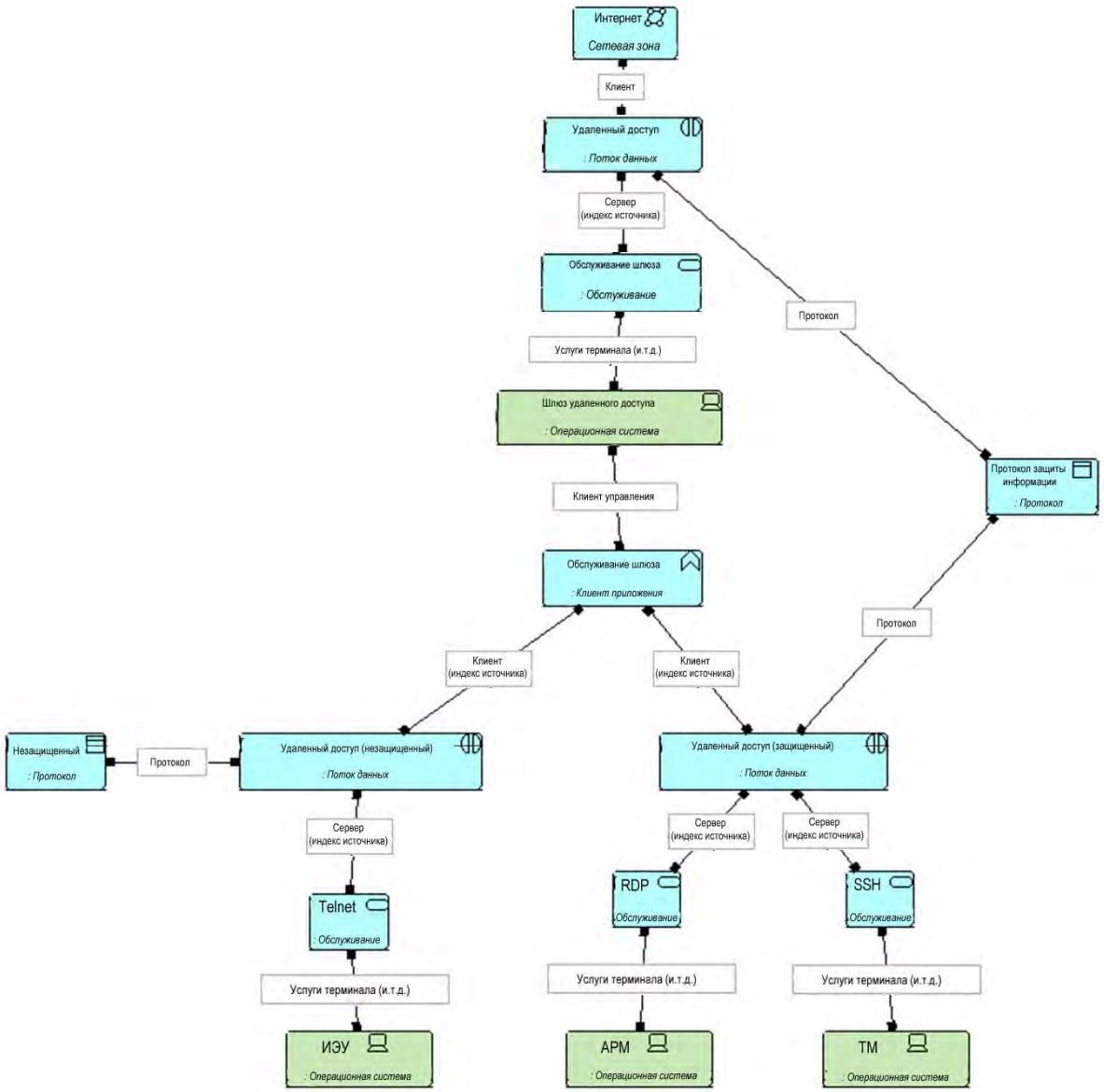



**Рисунок L-19 Общая схема удаленного доступа к оборудованию системы защиты и управления из внутренней сети**

### L.2.4 Роли персонала систем защиты и управления, учетные записи и программные сервисы

На рисунке L-20 показан обзор персонала, которому необходимо получить доступ к сети системы защиты и управления. Учетные данные определяют уровень доступа и привилегии по отношению к компонентам системы защиты и управления. Смоделировано две категории персонала, разделенных по ролям: *технический специалист* и *пользователь*. У обеих имеются равные права доступа. Они различаются тем, каким конечным устройством пользуются (АРМ или личный ноутбук).

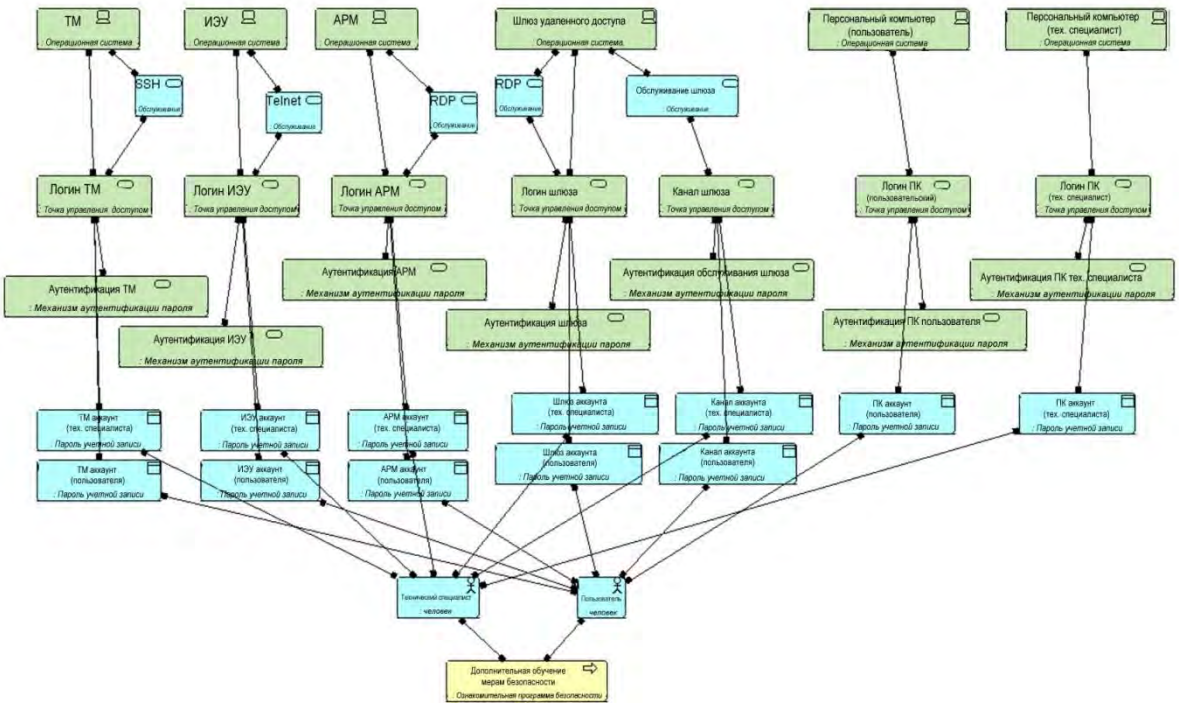



**Рис. L-20 Роли персонала системы защиты и управления, учетные записи и программные средства**

### L.2.5 Описание программного обеспечения в сети системы защиты и управления

На рисунке L-21 представлено описание программного обеспечения в системе защиты и управления. Модель содержит четыре операционные системы: VxWorks, Windows XP Service Pack 3, Windows CE и Windows 7.

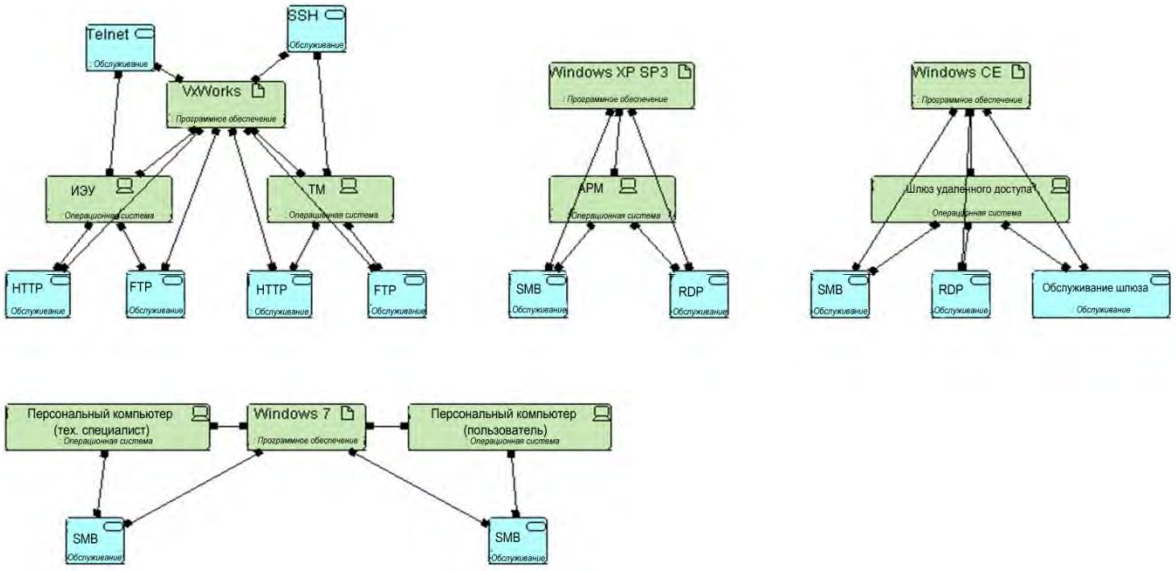



**Рис. L-21 Описание программного обеспечения в сети системы защиты и управления**

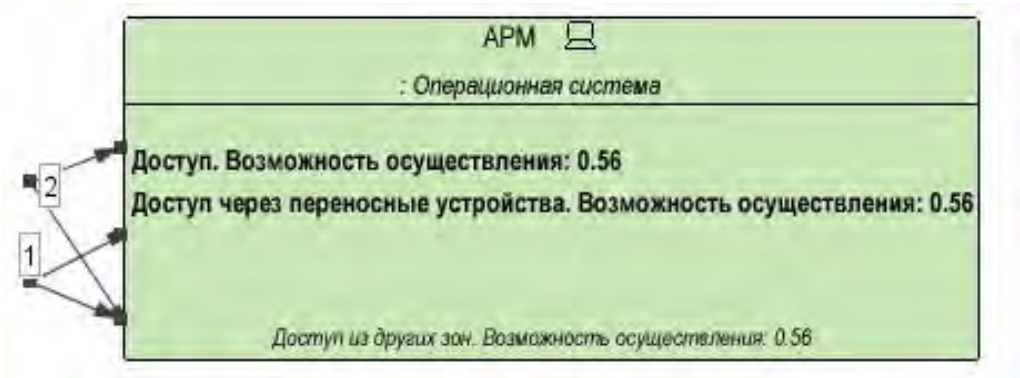
## L.3 Сценарии кибератак

### L.3.1 Сценарий атаки №1 (стандарт)

Задача: получить доступ к АРМ через USB

Технический подход: Злоумышленник устанавливает несколько USB накопителей за пределами зоны системы защиты и управления. Ничего не подозревающий пользователь вставляет один из них в АРМ.

Результаты расчета CySeMoL:



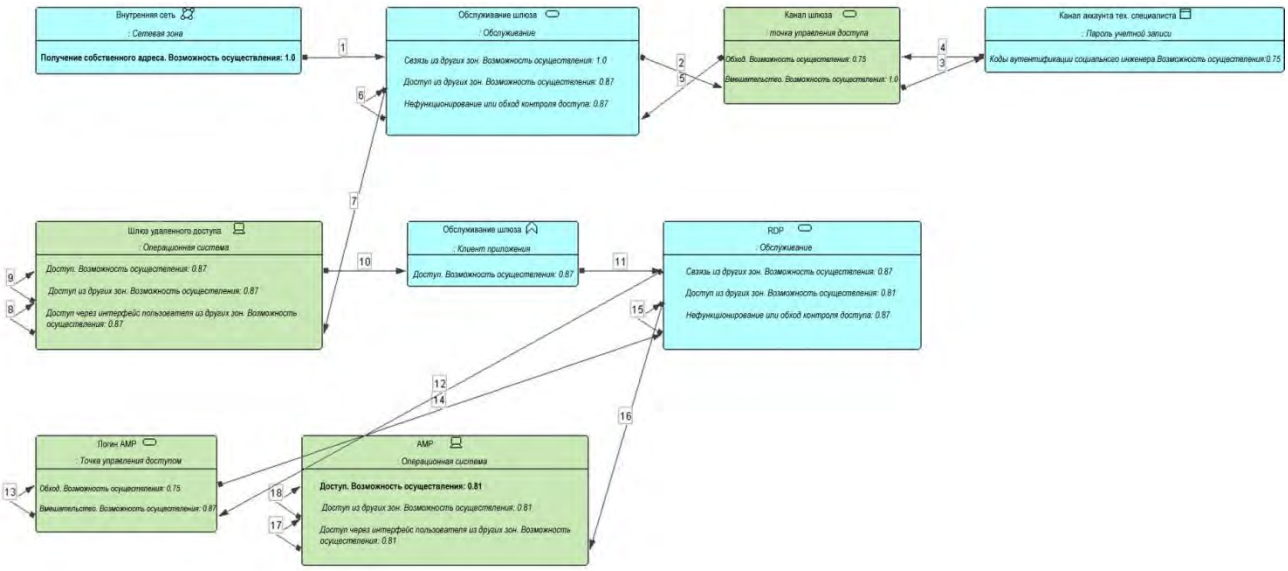

Примечания:
Вероятность успешного взлома: 56%
**Предложение по противодействию**: Отключить все USB накопители.
Новая вероятность успешного взлома: 0%.

### L.3.2 Сценарий атаки №2 (USB накопители отключены)

Задача: Так как злоумышленник не может использовать USB накопители, то наиболее вероятным способом проведения атаки будет получение обманным путем учетных данных у работника, не прошедшего обучение мерам безопасности (злоумышленник пользуется Интернетом и удаленным соединением).

Технический подход: Злоумышленник обманным путем вынуждает технического специалиста предоставить ему его/её учетные данные и использует их для получения удаленного доступа к АРМ (через шлюз удаленного доступа).

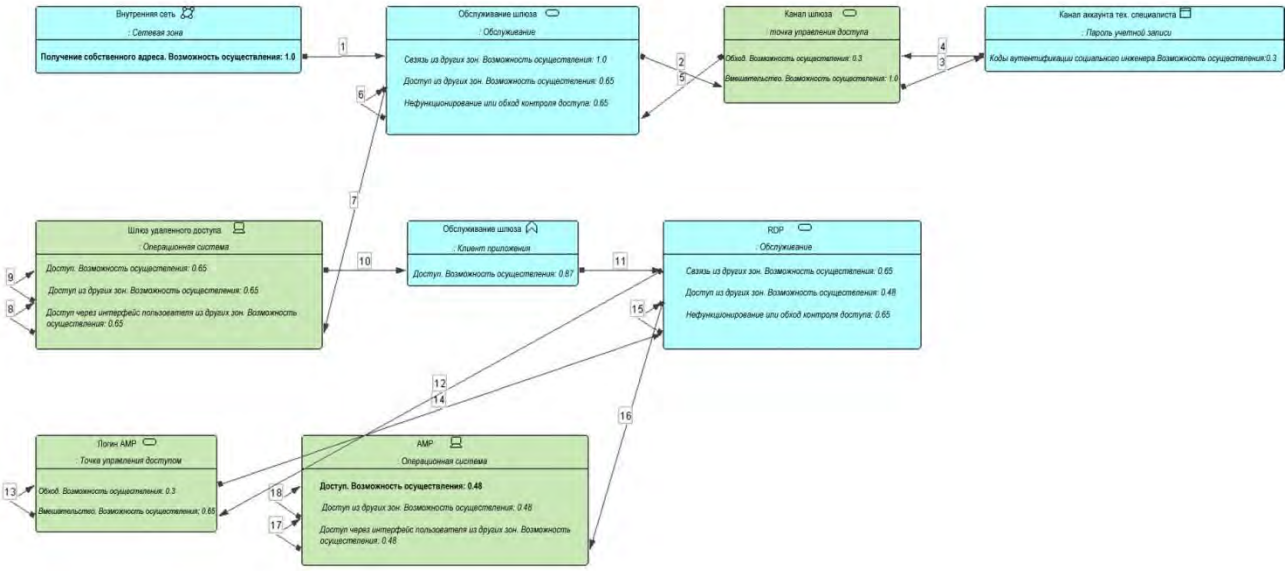
Модель CySeMoL:




Вероятность успешного взлома: 81%

**Рекомендации по противодействию**: Подготовка технического персонала, компетентного в аспектах безопасности.

Модель CySeMoL:




Новая вероятность успешного взлома: 48%

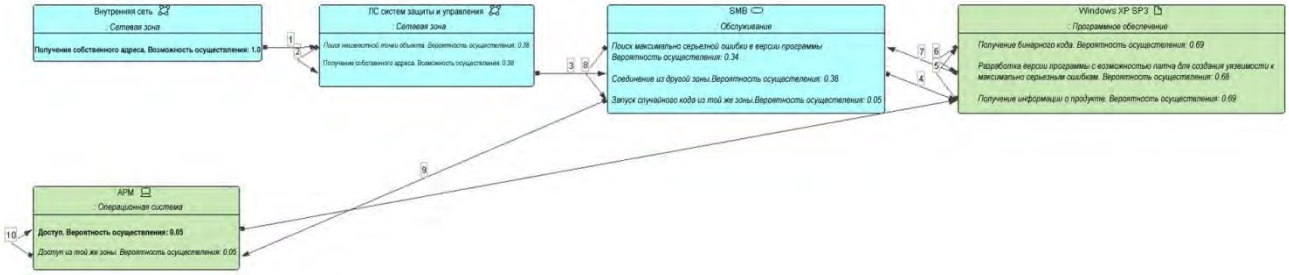
### L.3.3 Сценарий атаки №3 (USB-носитель отключен, персонал проинформирован)

**Задача**: Если злоумышленник не в состоянии воспользоваться USB-накопителем, а технический персонал подготовлен к борьбе со взломщиками, тогда взлом можно произвести через использование специальных программ для получения доступа к АРМ.

Технический подход: Злоумышленник находит ошибки в системе сетевой защиты компьютера и с помощью адреса во внешней сети на специальную программу получает доступ к АРМ и исследует их на предмет наличия уязвимостей. Злоумышленник обнаруживает уязвимость ПО без

необходимых патчей, такое ПО поддается взлому через современные хакерские программы (подробная информация доступна в интернете), необходима лишь последняя версия подобной программы.

Модель CySeMoL:

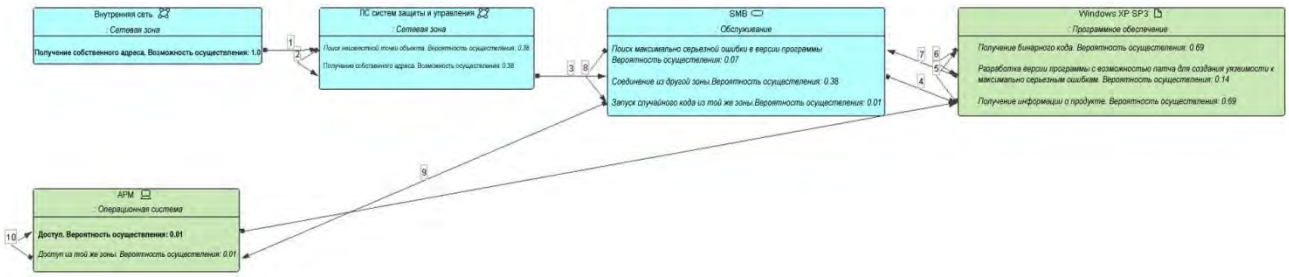



Вероятность успешного взлома: 5%

**Рекомендации по борьбе:** ввести автоматическое управление патчей в систему релейной защиты и управления.

Технический подход: Злоумышленник находит ошибки в системе сетевой защиты компьютера и с помощью адреса во внешней сети на специальную программу получает доступ к АРМ и исследует их на предмет наличия уязвимостей. Поскольку АРМ содержит полностью обновленные патчи и не допустит утечек информации по незащищенным каналам, взломщик решает вернуть систему к состоянию нулевого дня для получения в ней особых привелегий (подробнее см. нулевой день для MS Windows SP3)

Модель CySeMoL:




Новая вероятность успешного взлома: 1%.

# Приложение M
# Жизненный цикл управления ключами

## M.1 Введение в управление ключами

В криптографии управление ключами включает все положения криптографических протоколов системы шифрования, команд пользователя и т.п. Эти положения включают в себя создание, обмен, хранение, охрану, использование, проверку и замену ключей. Успешное управление ключами имеет огромное значение для защиты криптографической системы и обеспечивает защиту и контроль конфиденциальности данных, в некоторых случаях – целостности данных. Управление ключами осуществляется не только инженерами релейной защиты и управления. Напротив, инженеры релейной защиты и управления представляют только часть персонала по управлению ключами, они отвечают за принцип работы вспомогательных функций управления ключами, которые имеют непосредственное отношение к системам релейной защиты и управления, их подсистемам и компонентам, в которых для защиты используются ключи.

Для осуществления эффективной защиты и контроля ключей, инженеры релейной защиты и управления должны быть ознакомлены со следующей технической спецификацией: NIST SP 800-55[59], NIST SP 800-57[62], и ANSI X9.69[63]. Задача публикаций NIST заключается в определении эффективных путей защиты целостности ключей. Задача стандарта ANSI состоит в расширении системы управления ключами для повышения ее эффективности.

## M.2 Формы ключей

Существуют различные виды ключей; ассиметричные, симметричные, комбинированные. Принцип работы ключей основан на математических алгоритмах, которые они поддерживают.

- Для асимметричных ключей обычно используются алгоритмы RSA[22], эллиптическая кривая[23] и алгоритм Диффи-Хеллмена[24].

- *Для симметричных ключей обычно используются хэш-алгоритмы и алгоритмы шифрования данных, такие как Triple DES25[25] или передовой стандарт шифрования.

## M.3 Жизненный цикл использования ключевого материала

### A.3.1 Введение в жизненный цикл ключей

Понимание процесса управления ключами требует представления о сроках эксплуатации ключей, являющихся его неотъемлемой частью. Ключ представляет собой информационный фрагмент, изменяющий механизм алгоритма шифрования. Перед использованием таких механизмов в шифровании сообщений системы релейной защиты и управления или фрагментов информации выбирается ключ. Без информации о ключе расшифровка получаемых данных в какую-либо доступную человеку или машине форму практически невозможна.

Жизненный цикл ключа начинается с периода действия шифра, описывающего основные этапы жизни ключа, от создания до аннулирования и утилизации системы релейной защиты и

[22] Рон Ривест, Ади Шамир и Леонард Адельман из MIT публично описали алгоритм в 1977; буквы в названии происходят от их фамилий, перечисленных в том же порядке, что предложен выше.

[23] Шифрование эллиптической кривой (ECC) – подход к шифрованию открытого ключа, основанный на алгебраической структуре эллиптических кривых по конечным областям. Нил Коблиц и Виктор С. Миллер предложили использовать данный метод в 1985.

[24] Для установки общего секретного ключа для двухстороннего пользования без предварительного знакомства сторон используют обмен зашифрованными ключами Диффи Хеллмена по незащищённому каналу связи. Эти ключи используются для шифровки сообщений с использованием симметричного ключевого шифра.

[25] В шифровании Triple DES – общее название для блочного шифра Triple Data Encryption Algorithm (TDEA) – см. SP NIST 800-57 и 18033-3:2005 ISO/IEC.

управления работает в режиме 24/7,и зависит от постоянного доступа к важным коммуникационным ресурсам. На рисунке М-22 проиллюстрирована схема расположения ключей в пусковых системах.

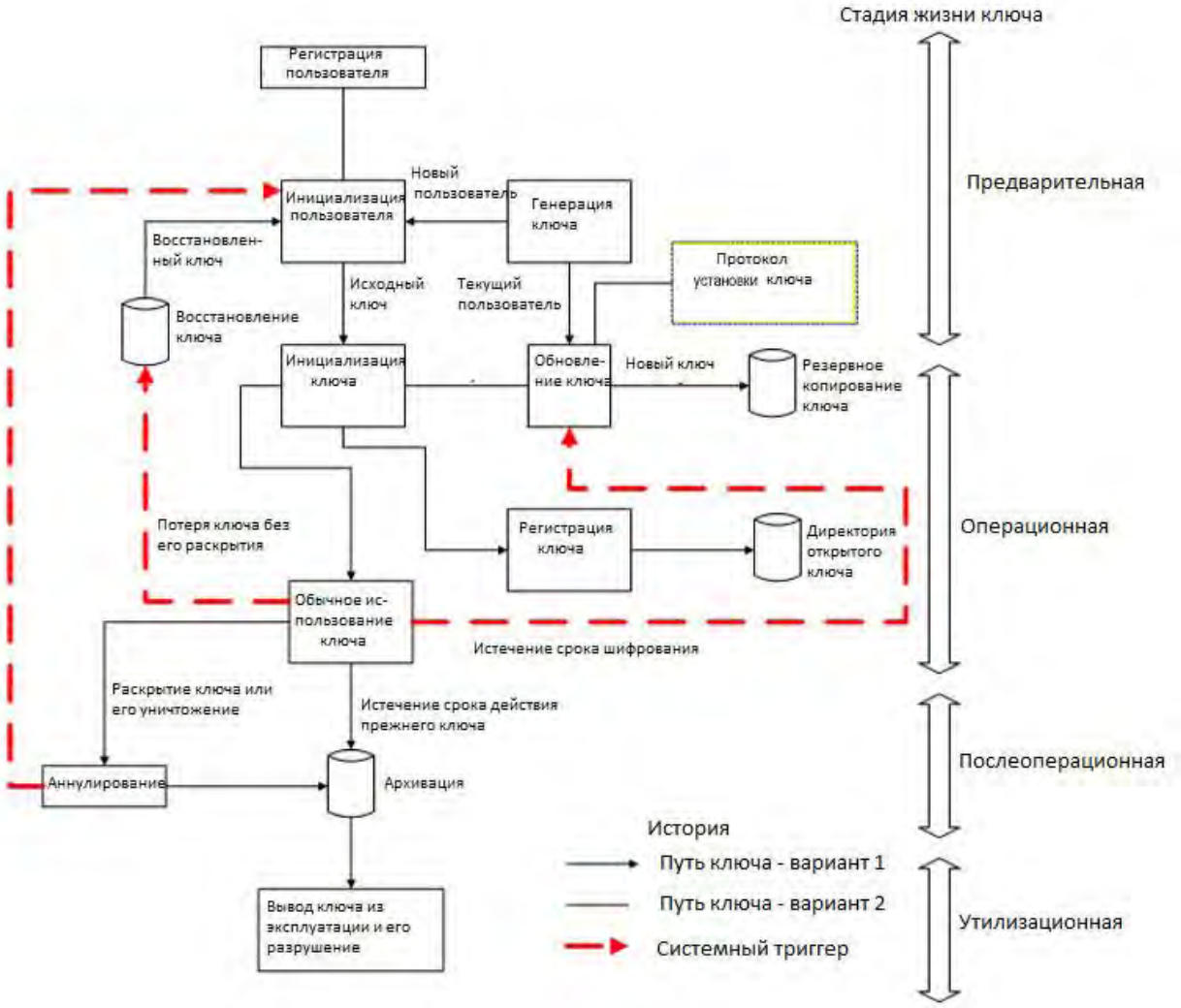



**Рисунок М-22 Цикл управления ключами**

### М.3.2 Генерация и распространение ключей

Для сохранения секретности информации и поддержания работы системы релейной защиты и управления в режиме 24/7, необходимо генерировать и распространять ключи. Схема или система управления ключами эффективна только тогда, когда что-то (как правило сам код ключа, но может быть и алгоритм шифрования) остается секретным. Сохранение секретности информации является очень непростой задачей, особенно с учетом географической распространённости оперативных органов релейной защиты и управления. Таким образом, формирование ключа при условии, что ключ может иметь широкий или очень узкий спектр использования, приводит к определению эффективного канала распределения. Канал может быть физическим, таким как курьер и т.п. Существуют и электронные каналы, например интернет, но ему нельзя доверять. Требования к времени доставки, определяемые самыми важными составляющими оперативной работы релейной защиты и управления, требующей высокой степени безопасности, выявляют средства распределения ключей.

Кроме простейших операций системы релейной защиты и управления, где компоненты ключа остаются неизменными на протяжении всего срока их службы, ключи требуются и в период шифрования. Эти ключи следует периодически обновлять. Время использования ключей может быть разным. Период шифрования определяется временем, в течение которого ключ

действителен и законно используется физическим или юридическим лицом. Период шифрования данных служит для:

- Ограничения информации (связанной с конкретным ключом) доступной для анализа шифра;
- Ограничение утечки информации в случае рассекречивания одного из ключей;
- Ограничение использования конкретной технологии ее предполагаемым эффективным сроком эксплуатации;
- Ограничение времени, в течение которого может быть осуществлена интенсивная хакерская атака (в приложениях ПСАУ, где долгосрочная ключевая защита не требуется).

### M.3.3 Стадии жизни ключа

Работа устройств системы релейной защиты и управления предполагает безопасное управление ключевым материалом на протяжении всех стадий использования, показанных на рисунке M-22: преоперационная, операционная, постоперационная и утилизационная. Кроме того, система управления ключами должна обеспечивать защищенность используемых ключей. Управление резервными копиями ключей и их восстановление крайне важно для обеспечения работы в круглосуточном режиме в случаях, когда система управления первичным ключом неисправна либо отключена.

## M.4 Требования ПСАУ, влияющие на схемы управления ключами

Оперативная работа релейной защиты и управления должна осуществляться в режиме 24/7. Безопасность, которую обеспечивает шифрование данных, должна быть эффективной и понятной для большинства функций, осуществляемых системами релейной защиты и управления. Это накладывает очень строгие ограничения к выбору схем управления ключами. Данное приложение описывает варианты выбора этих схем с помощью схемы CKM[26].

### M.4.1 Защита информации и канала передачи данных

Шифрование информации осуществляется через специальные защищенные сетевые каналы системы релейной защиты и управления, либо непосредственно через шифрование передаваемой информации. Системы релейной защиты и управления зачастую приходится выполнять таким образом, что применяется и зашифрованный канал, и шифрование самих данных. Как правило, защищенный канал работает по протоколу частной виртуальной сети (VPN). Таким образом, протокол VPN становится ключевой архитектурой при использовании симметричной схемы CKM. Кроме защиты канала, защита данных системы релейной защиты и управления (содержания), таких как настройки IED, может быть расширена до непосредственного манипулирования содержанием. В зависимости от требований архитектуры могут быть использованы как симметричные, так и асимметричные схемы CKM. Различия этих типов схем состоят в выборе алгоритма идентификации данных.

### M.4.2 Ролевой доступ к включению механизмов управления

CKM расшифровывается как создание ключа для каждого сообщения. Ключ для шифрования сообщений (текущий) создается по мере необходимости автором сообщения и может быть восстановлен только специальными средствами, обладатели которых имеют право на расшифровку и анализ содержания.

Схема CKM включает в себя несколько компонентов, являющихся важными с точки зрения эффективности и понятности:

[26] CKM является зарегистрированной торговой маркой компании Tecsec, Inc. Tecsec дала разрешение использовать их данные в информативном приложении этой технической характеристики.

1) разбиение ключей в произвольном порядке для вариативности,
2) симметрично разделенные ключи для определения границ шифрования, связанного с архитектурным сегментом системы релейной защиты и управления подстанции, для обновления шифрования на сетевом уровне без необходимости изменять механизмы шифрования, привязанные к сообщению[27] и
3) ассиметрично разделенные ключи, привязывающие шифрование к контролю доступа к содержанию сообщения.

Схема CKM также может включать проверку целостности содержания сообщений, использующую алгоритм защиты хеша (A3X).

Для функционирования системы релейной защиты и управления требуется контроль доступа, основанный на дифференциации ролей. Поэтому необходимо устанавливать права доступа к содержанию на основе ролей, правил или другой информации, в зависимости от представления. Использование ролевой системы контроля доступа к сообщениям обеспечивает возможность увеличения количества операций в системы релейной защиты и управления, обслуживающего персонала и событий, имеющих доступ в соответствии с ролями. Схема всегда должна определять роль пользователя, даже если на одну и ту же роль назначают разных людей. Идентификационные данные или идентификатор определяют роль пользователя. Идентификационные данные остаются в обращении вместе с ролью или иными обозначениями.

При использовании ролей схема CKM особенно полезна, когда сообщения проходят через группы неизвестных отправителю пользователей в течение долгого времени, и способна обеспечить защиту информации о длительном состоянии, не требующей запоминания. Эта ситуация является одной из типовых для распространённой системы релейной защиты и управления.

В схеме CKM процесс шифрования является закрытым и зависит от создания и жизненного цикла разделения ключа в процессе администрирования (см. рис. М-22). Идентификационные данные напрямую связаны с набором асимметричных ключей. Этот набор отделяет права чтения от прав записи – асимметрично разделенный открытый ключ для записи и асимметричный разделенный закрытый ключ для чтения. Ассиметричный разделенный ключ может быть введен в действие по алгоритму Диффи-Хэлмана с динамическим значением или динамической эллиптической кривой[28].

Соединение компонентов и симметричного алгоритма дает возможность рассматривать схему CKM как набор модулей, который может предоставить различный доступ авторизированным пользователям. Например, для ряда компонентов получаемое сообщение будет зашифровано в соответствии с симметричным алгоритмом, используемым в данный момент. Сам алгоритм может меняться, вследствие чего изменится и шифр. Таким образом, симметричный алгоритм охватывает все сообщение, само же сообщение является математически независимым от результатов прочих симметричных алгоритмов.

Контроль доступа на основе ролевой дифференциации с применением механизмов, описанных в приложении, дает возможность удовлетворить основным требованиям идентификации и аутентификации, а также контролировать любой объект системы релейной защиты и управления.

### М.4.3 Предварительное размещение разделенных ключей

В процессе администрирования симметричные и ассиметричные разделенные ключи предварительно размещают так, как показано на рисунке М-22. Обеспечение энтропии[29] в процессе комбинирования разделенных ключей достигается посредствам создания произвольного разделенного ключа. Зашифрованное сообщение отправляется адресатам, имеющим идентичное значение ключа для расшифровки сообщения. Для этого зашифрованное сообщение принудительно отправляется на иерархическое распределение для выборочной расшифровки

[27] При выборе схемы систем защиты и управления, оценка альтернатив предполагает понимание их воздействия на работу систем защиты и управления в связи с потребностью смены шифровальных средств управления, связанных сообщением.
[28] Открытые ключи бывают двух видов: однодневные и постоянные (причем надежные согласно сертификату). Подтверждение подлинности постоянных ключей не требуется.
[29] Энтропия – мера эффективности.

только определенными группами, и для воссоздания рабочего ключа используются предопределенные возможности разделенных ключей и СКМ схемы. Данный способ распределения – не самый надежный.

Для создания ключа шифрования сообщений математически комбинируются симметричный и ассиметричный ключи. Рекомендуемый подход предполагает обмен ключами как составную часть управления ими по протоколу администрирования и локальное хранение ключей в базе информации управления безопасностью (БИУБ). Это значит, что ключ шифрования сообщений можно восстановить, и соответствующий получатель может всегда расшифровать сообщение.

### М.4.4 Предотвращение остаточного шифрования сообщения

Строка заголовка СКМ – открытый пакет информации, необходимой для воссоздания рабочего ключа СКМ. Также строка заголовка СКМ может быть частью более крупной системы безопасности с СКМ шифрованием, включающей протоколы ключей и прочие кодовые элементы целостности. Данные, хранимые в строке заголовка СКМ включают в себя:

- информация идентификации домена, определяющая домен защиты, необходимый для корректной расшифровки данных,
- перечень идентификационных данных, определяющих идентификаторы СКМ для создания рабочего ключа,
- идентификатор алгоритма шифрования,
- эфемерный открытый ключ,
- зашифрованное случайное значение.

Все эти компоненты, плюс устройство идентификации, содержащее обозначение домена и идентификационные данные, обеспечивают возможность воссоздания рабочего ключа СКМ. Для обеспечения целостности заголовка при обработке чувствительных функций заголовка используются подписи или схемы сетевого шифрования.

Как только шифрование сообщения завершено, необходимо уничтожить ключ шифрования сообщения. Расшифровка сообщения может состояться только через процесс сборки. Схема СКМ запускает динамическое создание ключа шифрования сообщения, что не приводит к остаточной шифровке сообщения.

### М.4.5 Обеспечение разделения данных

Особенностью системы релейной защиты и управления является широкая область ее применения и расположение в георграфически удаленных друг от друга точках. Для эффективной работы требуется своевременная передача данных. Эффективность реализуется особыми механизмами, доступными благодаря безопасному использованию разделения данных

Схема СКМ дает возможность реализовать разделение данных путем шифрования в целях контроля доступа и защиты содержания данных. В подходе совмещаются метод разделения ключа (с соответствующими идентификационными данными, представляющими различные категории доступа, прописанные в уставе организации) с алгоритмом симметричного шифрования для создания ключа шифрования сообщения в целях зашифровки или расшифровки. Обычно используется некоторый набор предварительно размещенных разделенных ключей. Комбинирование этих разделенных ключей со случайным разбиением гарантирует создание уникального ключа шифрования для каждого сообщения. Процедура должна выполнить случайное разделение к моменту, когда сообщение будет подготовлено к шифрованию.

Для широкого круга операций системы релейной защиты и управления преимущества данного подхода заключаются в простоте понимания, управления, степени детализации и эффективности процесса по сравнению с традиционными подходами со статическими ключами. Например, возможно создание набора нескольких ключей шифрования сообщений таким образом, чтобы все содержание сообщения представляло собой отдельные зашифрованные сообщения. Доступ к зашифрованным файлам может быть различным и зависит от учетной записи пользователя.

Асимметричные разделенные ключи, связывающие шифрование контроля доступа с содержанием сообщения могут также быть симметричными разделенными ключами. Процедура комбинирует непосредственно симметричные разделения ключей, используя, например, алгоритм защищенного хеширования. Преимущество асимметричного разделенного ключа состоит в использовании открытого и закрытого ключа для чтения и записи по отдельности. Данная особенность позволяет использовать механизмы контроля, встроенные в системы релейной защиты и управления, их подсистемы и компоненты.

### M.4.6 Эффективные варианты аннулирования

Для множества систем релейной защиты и управления, охватывающих большие области, и особенно для тех, которые пересекают национальные границы, существует централизованная политика безопасности для организации управления ключами на местном уровне. Важное значение имеют ограничения, наложенные на сроки аннулирования ключей.

В пределах структуры CKM существует несколько методов для аннулирования. Варианты аннулирования заключаются в изменении одного или нескольких разделенных ключей, либо в отмене устройства идентификации схемы. С точки зрения системы, структура CKM позволяет аннулировать цифровую подпись через схему PKI или с помощью функции вне рамок схемы CKM. Механика схемы CKM также предполагает возможность изменения некоторого числа разбиений ключей.

Если схема CKM находится в режиме офф-лайн (не подключена к сети), аннулирование разбиений в реальном времени становится невыгодным; однако, возможно аннулирование через привязку времени жизни ключа и его материалов к устройству идентификации. Механизм администрирования допускает очень грубый либо детальный контроль жизни всех идентификационных данных и каждого разделенного ключа. Это может осуществляться на всех уровнях и во всех областях системы релейной защиты и управления. Сюда относятся как объекты систем релейной защиты и управления, так и внешние предприятия, взаимодействующие с коммуникациями систем релейной защиты и управления.

#### M.4.6.1 Замена разделенных ключей

Установленные в системе релейной защиты и управления симметричные разделенные ключи могут участвовать в процессе аннулировании. Эти ключи непосредственно относятся к конечному ключу шифрования, а значит смена такого ключа приводит к появлению нового ключа шифрования. Однако, инженер систем релейной защиты и управления должен быть в курсе, что такая замена может повлиять на все зашифрованные сообщения или их содержание, если замена происходит на уровне всего предприятия.

В форме разделенных ключей также выступают идентификационные данные, которые также могут участвовать в процессе аннулирования. Замена этих разделений ключей влияет на сообщения или файлы, защищенные информацией или данными, имеющие непосредственное отношения к этим идентификационным данным.

Процесс аннулирования должен быть включен в административный цикл управления этими разделенными ключами.

#### M.4.6.2 Аннулирование устройства идентификации схемы CKM

Устройство идентификации является одним из основных элементов в управлении разделенными ключами и прочими уязвимыми данными. Оно может иметь форму программного обеспечения или устройства аппаратного обеспечения, например смарт-карты. Оно может включать уникальные закономерности, подлежащие аннулированию. Управление структурой должна иметь одну или несколько таких уникальных закономерностей, подлежащих изменениям в зависимости от внешней политики компании.

#### M.4.6.3 Аннулирование цифровой подписи

Архитектура схемы CKM и строка заголовка предполагают возможность включения цифровой подписи или протокола открытого ключа. Возможно аннулирование такого протокола через поддержку PKI. Если PKI недоступна, следует расширять саму схему CKM добавлением цифровой подписи с аннулированием признаков, найденных в разделенном ключе, которые могут повлиять на создание новой цифровой подписи. В данном случае административная структура предполагала бы раздельное распределение подписей, которое в дальнейшем вызвало бы замену разделенных ключей.

### M.4.6.4 Запрос о комментариях (RFC) 3647

В RFC 3647 (ноябрь 2003 года) предлагается концепция написания сертификатов и положения сертификации (CPS). В ноябре 2006, [американская] Федеральная служба сертификации открытых ключей (ФССОК) рекомендовала предприятиям, сертифицированным в соответствии с федеральным объединенным центром сертификации (ФОЦС), принять меры в соответствии с RFC 3647 в течение одного года. Это требование относится к федеральным агентствам. Теперь множество операторов управления ключами (в стране и за ее пределами) публикуют положения о различных мероприятиях в соответствии с RFC 3647. Анализ таких публикаций позволит оценить благонадежность предоставляемых услуг в сфере управления ключами.

## M.5 Работа ПСАУ требует эластичное управление ключами

Эластичность – способность поддерживать работоспособность на платформах разных уровней, отличающихся возможностями и скоростью работы.

Динамическая схема CKM крайне эластична, особенно когда используется для защиты данных систем релейной защиты и управления. Доступ к информации систем релейной защиты и управления контролируется с помощью устройства идентификации, которое не требует соединения с центральным хранилищем или сервером для повышения эффективности шифрования. Ограничения пропускной способности, связанные с центральным сервером, снимаются, как только клиент систем релейной защиты и управления регистрируется в качестве администратора. Задача защиты и шифрования ложится на клиента, который выполняет процессы распределения и защиты данных. Если политика предполагает, что центральный сервер является частью архитектуры[30], использующей периодическое соединение, постоянное вмешательство сервера не требуется.

В системе CKM модули администрирования участников, устройств идентификации и разделения ключей для логических групп пользователей являются частями сегментированной зоны систем релейной защиты и управления. Увеличение вычислительной мощности при обработке модулей обеспечивает эластичность. Эти серверы выполняют основную часть операций шифрования, требующихся для создания и защиты разделенных ключей, самостоятельно.

Серверы соединяются с одной или несколькими базами данных, сохраняющими историю шифрования объектов текущих или бывших модулей предприятия. База данных может находиться на одном сервере, либо на сгруппированных серверах, в зависимости от требуемой производительности и географической удалённости элементов системы релейной защиты и управления. Агенты в форме программ могут выполнять административные функции для задач автоматизации под административным надзором, что, в дополнение, должно увеличивать производительность. Авторизация через административный контроль обеспечивает надежное управление агентами и их использование.

Администрация структуры CKM предлагает двойственный подход к распознанию топографии коммуникационной сети системы релейной защиты и управления с распознанием правил и ролей. Процедура заключается в использовании повторения модели потока информации оперативной работы систем релейной защиты и управления и операций по управлению. Изменения правил и ролей для модулей CKM все еще сохраняют соответствующий доступ к истории данных. Выбранный разделенный ключ является заменяемым, при условии что существует не один временной участок, связанный с разделенным ключом. Изменение прав доступа через

[30] Раздел 2-1 данного стандарта не предполагает, что центральный сервер являлся частью общей архитектуры.

идентификационные данные на уровне каждого участника обеспечивает еще большую универсальность с помощью распределения контроля управления. Это достигается через создание виртуального повторения для физического доступа к информации систем релейной защиты и управления и ИЭУ (терминалам системы релейной защиты и управления).

Разделенные ключи могут быть заменены, обновлены или аннулированы без влияния на информационную структуру или структурную схему обработки данных в системе релейной защиты и управления. Независимость схемы СКМ и инфраструктуры систем релейной защиты и управления приводит к повышению пропускной способности без влияния на ресурсы друг друга.

Данная возможность предоставляется для использования модулей СКМ на разных операционных системах, чтобы добиться расширения базы приложений программного и аппаратного обеспечения.

Симметричная структура шифрования СКМ предполагает многоуровневую систему, включающую уровень клиента, сервера и базы данных. Каждый уровень может быть независимо расширен за счет дополнительных ресурсов для того, чтобы реализовать новые возможности. Внедрение связи посредством виртуальных ключей с отдельными зонами системы релейной защиты и управления и внешними интерфейсными зонами, которые состоят из собственных модулей СКМ, должно расширить контроль информации наряду с расширением количества процессов, протекающих в различных крупных системах.

# Приложение N
# Опасные последствия в системах защиты и управления и схемах защиты целостности системы (SIPS)

## N.1 Вступление

Для инженеров релейной защиты представляют интерес возможные последствия в случае успешной кибератаки на системы релейной защиты и управления и на системы SIPS, входящие в состав общей электроэнергетической системы. Главными задачами электроэнергетической системы общего пользования являются поддержание работы и минимизация последствий внутрисетевых сбоев с целью обеспечения потребителей надежной и качественной электроэнергией.

Для достижения этого в электроэнергетических системах должно контролироваться множество факторов, таких как частота, напряжение, коэффициент мощности, обмен электроэнергией с соседними системами энергоснабжения и многие другие. Кроме того, в целях поддержания устойчивости и стабильности сети устанавливается цифровая релейная защита, которая является ИЭУ. Она обеспечивает защиту основного электрического оборудования сети от электрических сбоев, которые должны быть устранены за допустимый временной промежуток (от трех до шести циклов энергосистемы).

Функции и стоимость оборудования всегда являются определяющими факторами уровня защиты кибербезопасности. Для такого оборудования, как силовые трансформаторы и генераторы, используется адаптивная защита, способная реагировать на ток нагрузки. Для линий, главным аспектом является стабильность сети (максимально быстрое аварийное отключение при возникновении неисправности на ЛЭП). Поэтому настройка и конфигурация цифровой релейной защиты должны быть точными и оптимальными, чтобы избежать проблем с безопасностью, таких как ложное аварийное отключение или отказ аварийного отключения в случае сбоя. По этой причине на главные генерирующие и передающие части энергосети устанавливаются двойные и даже тройные системы резервирующих защит.

Кроме того, системы SIPS все чаще используются в электроэнергетических системах общего пользования. Основная иерархическая структура систем SIPS, схем, используемых при восстановительных мероприятиях (RAS), и специальных схем защиты (SPS) показана на Рис. 23. Главное оборудование установлено в центре управления или на крупной подстанции, оно также может задействовать данные системы оперативно-диспетчерского управления или системы планирования и контроля энергопотребления. Элементы релейной защиты обеспечивают сохранность электрооборудования, а системы SIPS поддерживают стабильную работу энергетических сетей. Концепция схем защиты целостности системы — это обеспечение возможности поддержания стабильной работы сети при чрезвычайных событиях, таких как потеря более чем одной линии, отключение подстанции или электростанций. С точки зрения динамической устойчивости, системы такого рода должны обладать быстродействием, чтобы избегать потерь синхронизма генерирующих станций и препятствовать распространению возмущений по всей электрической сети. Как и устройства релейной защиты, системы SIPS – это ИЭУ, настройки, конфигурация и программное обеспечение которых должны быть точными и оптимальными. Ошибки в конфигурации или программировании этих систем могут привести к целому ряду отключений, что влечет за собой крупное длительное нарушение энергоснабжения сети. [64]

В целях контроля и обеспечения непрерывной оценки функциональности и состояния цифровой релейной защиты и систем SIPS обслуживающему персоналу требуется удаленный доступ к этому оборудованию. Такие устройства обеспечивают инженеров по вопросам защиты ценными данными, такими как индикация событий и их осциллограммы, и позволяют оптимизировать требуемые характеристики ИЭУ, а также определять и находить неисправности электрооборудования сети. Вследствие этого, для обеспечения удаленного доступа обслуживающему персоналу и ИЭУ требуется коммуникационная сетевая производственно-техническая база. Поскольку системы SIPS и системные элементы расположены по всей сети, для

получения данных от местных и удаленных ИЭУ и схем защиты целостности системы, расположенных на отдаленных подстанциях электрической сети,

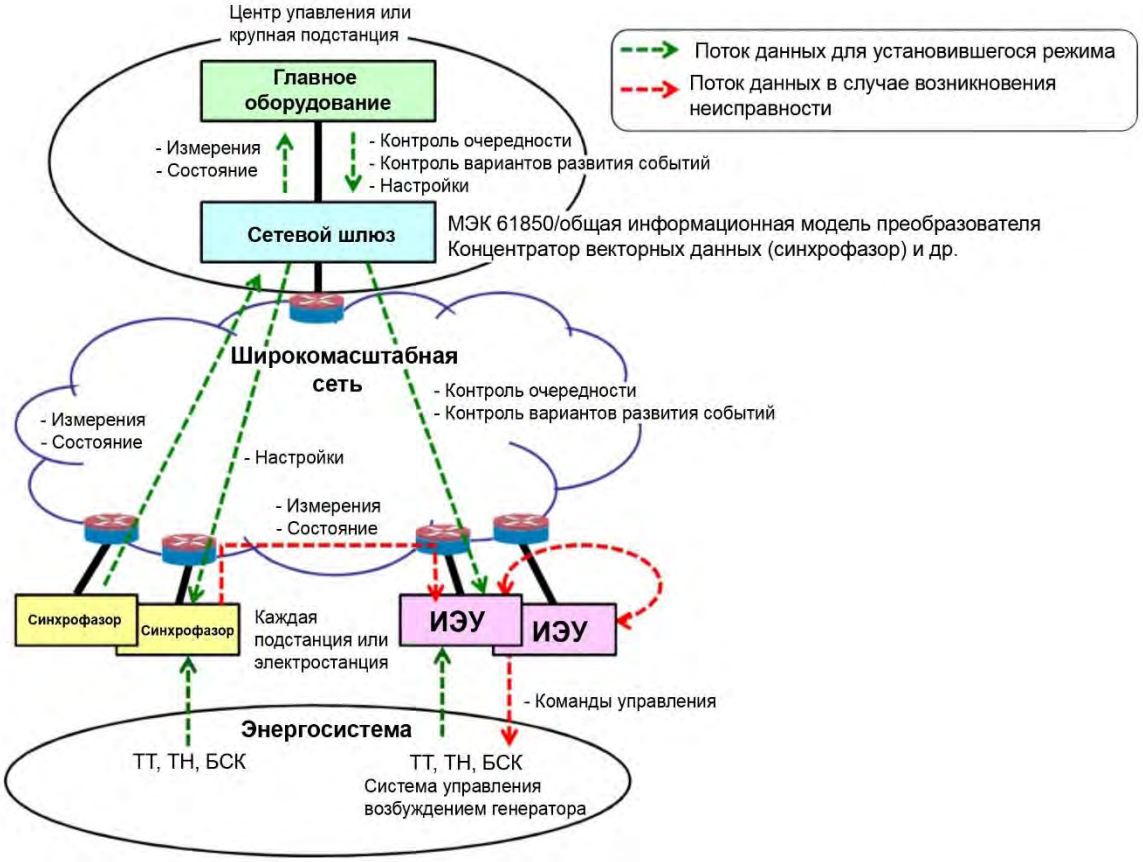



**Рисунок N-23 Основная иерархическая структура систем SIPS, RAS или SPS**

необходимо использование системы связи. В целях прекращения распространения повреждений и для предотвращения каскадных отключений, ИЭУ получают команду на аварийное отключение автоматического выключателя.

Однако коммуникационная производственно-техническая база и ИЭУ обладают рядом уязвимостей и создают предпосылки для многих угроз. Угрозы могут исходить как изнутри электроэнергетических систем общего пользования, так и извне. Например, сотрудники, обладающие физическим доступом к ИЭУ, могут непреднамеренно совершить действия, которые приведут к ошибкам в настройках, конфигурации или эксплуатации, что вызовет непроизвольные срабатывания реле или других ИЭУ. Злоумышленники в рядах персонала, а также среди других сотрудников таких как подрядчики, поставщики или производители, имеющие физический доступ к ИЭУ, также могут сбить настройки системы злонамеренно как непредумышленно, так и по многим другим причинам (экономическим, политическим, террористическим, как акт выражения злости и др.). Кроме того, использование сети связи создает большое разнообразие внешних угроз. Уязвимости из-за канала связи, прослушивание сети, подмена ID пользователя, сетевые атаки, вирусы, черви и многие другие угрозы могут принести значительный ущерб частям электроэнергетической системы общего пользования или даже вызвать длительное нарушение энергоснабжения сети.

Тяжесть последствий кибератаки на устройства релейной защиты и управления или ИЭУ сети зависит от того, на какую систему и оборудование была совершена атака. Например, тяжесть повреждений от успешной атаки на дифференциальные реле защиты силового трансформатора 700/300 кВ мощностью 1650 МВА намного значительнее по сравнению с повреждениями силового трансформатора 120/26.4 кВ мощностью 47 МВА. Кроме того, успешная атака на ПЛК (программируемый логический контроллер), являющийся частью системы SIPS, может повлиять на нагрузку, электростанцию и стабильность сети, что приведет к более серьезным последствиям по

сравнению с успешной атакой на релейную защиту линий.

Таким образом, в данной главе основное внимание уделяется воздействиям и последствиям успешных атак, совершаемых на цифровую релейную защиту и системы SIPS. Если при успешной кибератаке будет нарушена надежная работа релейной защиты, основному электрооборудованию может быть причинен серьезный ущерб. Кроме того, впоследствии в зависимости от тяжести его повреждения может быть нарушена устойчивость электрической сети.

## N.2 Предположение успешной атаки на цифровую релейную защиту

Рассмотрим электроэнергетическую систему общего пользования со слабой информационной защитой. Например, сеть подстанции не имеет системы управления паролями, таким образом, вполне вероятно, что пароль для всех ИЭУ одинаковый. Кроме того, в данной сети отсутствует шлюз безопасности, система сетевой защиты, зашифрованный канал передачи данных и нет системы аутентификации пользователей.

Такая ситуация обеспечивает хакеру простор для того, чтобы сбить настройки релейной защиты и поставить под угрозу стабильную работу электросети. Более того, даже постоянные или временные сотрудники, имеющие физический доступ к помещению главного щита управления подстанции, могут изменить настройки релейной защиты, причем без регистрации того, кто именно совершил данные изменения. Подобное отсутствие контроля и безопасности повышает риск возникновения потенциальных проблем, а их выявление и исправление становится очень трудоемким, особенно когда нет записи о том, кто вносил изменения в настройки и что именно было изменено в устройствах релейной защиты.

Конечно, на уровнях высокого напряжения схемы релейной защиты выполняют с резервированием. Например, на линии устанавливаются первичные и вторичные системы защиты, приобретенные у разных производителей или же имеющие разные алгоритмы работы. Традиционно, в электроэнергетической системе группы защит линий высокого напряжения с системой компенсации, состоящей из последовательно включенных конденсаторных батарей, разделяются как:

1) Первичная защита (система А);
2) Вторичная защита (система Б);
3) Резервные защиты и УРОВ (устройство резервирования отказов выключателей).

Как правило, ЛЭП в электроэнергетической системе защищаются с помощью двух различных систем защит (А и Б). Эти две системы работают параллельно и независимо друг от друга, что позволяет поддерживать защиту оборудования линии даже в случае выхода из строя одной из систем, а кроме того, выполнять запланированные мероприятия по обслуживанию. Защиты системы "А" не обязательно выполняют те же функции, что и "Б", для гарантии надежности используя оборудование от разных производителей. Кроме того, иногда к защите линии с системой компенсации, состоящей из последовательно включенных конденсаторных батарей, добавляется и другая защита, называемая резервной или местной резервной защитой. Это дистанционная защита и УРОВ, которая обеспечивает защиту второй линии в случае, когда основная защита срабатывает, однако выключатель поврежденной зоны не отключается.

Таким образом, вероятность того, что хакер может полностью нейтрализовать все системы защиты ЛЭП, снижается. Для этого он должен хорошо знать структуру, релейные схемы, марку, тип установленной релейной защиты и тому подобное. Конечно, сотрудники, работающие в компаниях электроэнергетической системы, могут иметь доступ к информации такого рода и предоставлять ее кибертеррористам.

В следующих пунктах будут рассмотрены последствия успешной атаки на цифровую релейную защиту, более детально затронуты вопросы стабильности сети, перетоков мощности по ЛЭП и ущерба, нанесенного электроэнергетической системе общего пользования. Рассматривая в качестве основного мотива кибертерроризм, злоумышленник может получить доступ к релейной защите электроэнергетической системы. Главный вопрос звучит следующим образом: каковы последствия для устойчивой работы электросети?

## N.3 Угроза защитам линии и ее влияние на энергосистему

В электрической сети присутствует множество источников емкостных и индуктивных эффектов. Различного рода резонансы могут усилить их до уровня, опасного для оборудования. В общем случае, топология сети хорошо контролируется и компенсируется в целях обеспечения устойчивой работы. Сеть должна выдерживать такие режимы, как:

- Потеря ЛЭП.
- Потеря источников, чьи производственные мощности не нарушают устойчивость сети.
- Снижение нагрузки, не нарушающее устойчивость или синхронизм.

Всякий раз, когда происходят более серьезные происшествия, устойчивая работа сети оказывается под угрозой. Следующие режимы являются наиболее тяжелыми:

- Потеря двух и более параллельных линий.
- Потеря линий и группы последовательно включенных конденсаторных батарей.
- Потеря источников или нагрузок, превышающая запас устойчивости.

Во время таких тяжелых режимов новая топология сети может быть либо слишком, либо недостаточно компенсирована. “Перекомпенсация” подразумевает значительное падение напряжения на нагрузке или в других точках сети, “недокомпенсация” – соответствующее повышение. Изменение напряжения влияет на энергопотребление, а оно, в свою очередь, влияет на устойчивость сети. Кроме того, перенапряжение – одна из главных проблем электросети. Чем длиннее линия, тем опаснее создание перенапряжения, оно может повредить или даже вывести из строя электрооборудование и ухудшить состояние сети, а также перенапряжение создает эксплуатационные ограничения передачи мощности.

На рисунке 24 представлены кривые зависимости напряжения от мощности. Этот график показывает влияние различных длин линий на зависимость напряжения от мощности. Например, напряжение на линии длиной 100 км является относительно нечувствительным к изменению мощности по сравнению с линиями большей длины. Кроме того, передаваемая на линии 100 км мощность выше по сравнению с мощностью линии длиной 600 км. Таким образом, сеть с ЛЭП значительной длины при сбоях является менее устойчивой, а при поддержании номинального напряжения позволяет передавать меньшую мощность.
Этот график представляет особый интерес тем, что показывает связь между двумя переменными, которые очень важны для контроля и управления в электрической сети. При изменении напряжения

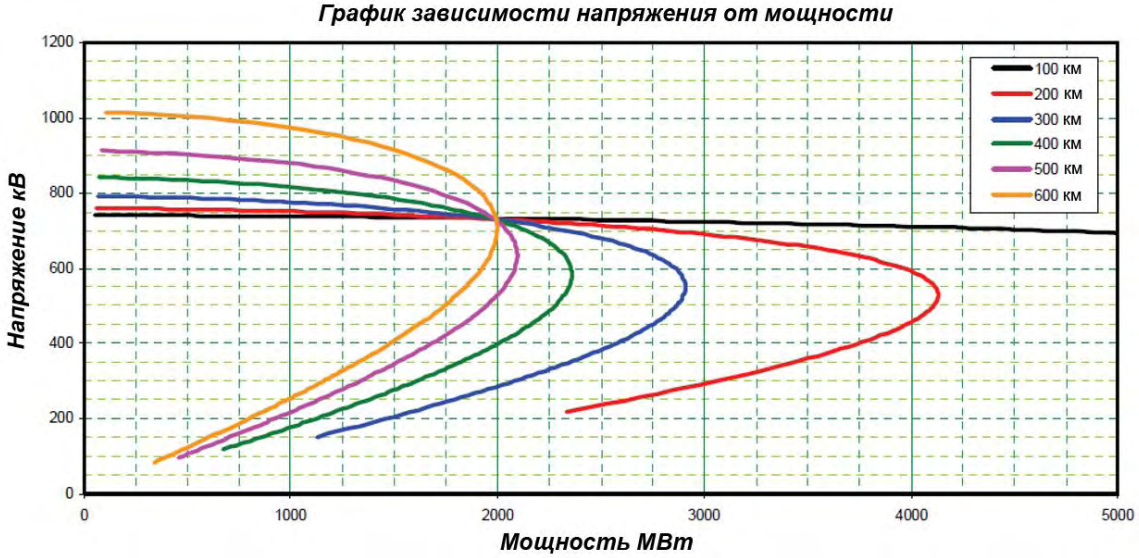



**Рисунок N-24 Типовые кривые зависимости напряжения от мощности**

сети меняется значение потребляемой мощности, а если при аварийной разгрузке энергосистемы изменится потребляемая мощность, то изменится и напряжение сети. Таким образом, между напряжением и мощностью существует взаимосвязь.

Кроме того, из рисунка 24 можно видеть, что большую мощность при сохранении номинального напряжения можно передавать  за счет использования нескольких параллельных линий. Серая линия – это кривая нагрузки; она пересекает кривые ЛЭП в точках равновесия сети (когда сеть устойчива). Номинальное напряжение (735 кВ) показано зеленой линией. В этом примере мы рассматриваем нагрузку в 5000 МВт на сеть 735 кВ. Для того, чтобы передать мощность 5000 МВт при сохранении номинального напряжения и поддержании устойчивости сети, мы должны использовать три параллельные линии. При потере одной или двух линий топология сети изменится, а точка равновесия переместится, существенно повлияв на напряжение и передаваемую мощность.

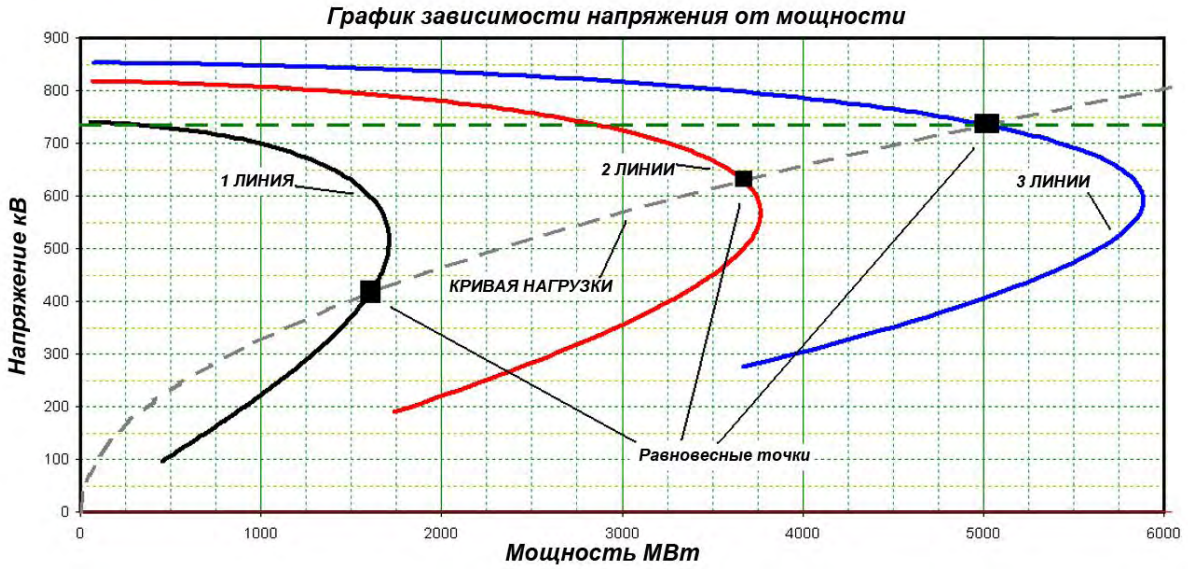



**Рисунок N-25  Кривая нагрузки на графике зависимости напряжения от мощности**

В этом примере топология сети изменилась, в работе остались две линии вместо трех. Это приводит к переносу точки равновесия в новое место, которому соответствует рабочее напряжение 650 кВ вместо 735 кВ и уровень передаваемой мощности в 3700 МВт вместо 5000 МВт. Хуже, если топология сети меняется с трех линий на одну. Рабочее напряжение составит 425 кВ вместо 735 кВ, уровень передаваемой мощности — 1600 МВт вместо 5000 МВт. Таким образом, число параллельных линий тоже влияет на напряжение и передаваемую мощность электрической сети.

Обратите внимание: если в работе остаются две линии вместо трех, можно достигнуть точки равновесия при сохранении номинального напряжения путем отключения нагрузки (см. рис. 26). Фактически, если мы снизим нагрузку на 2000 МВт, кривая нагрузки изменится. Новому положению равновесной точки будут соответствовать номинальное напряжение и нагрузка в 3000 МВт.

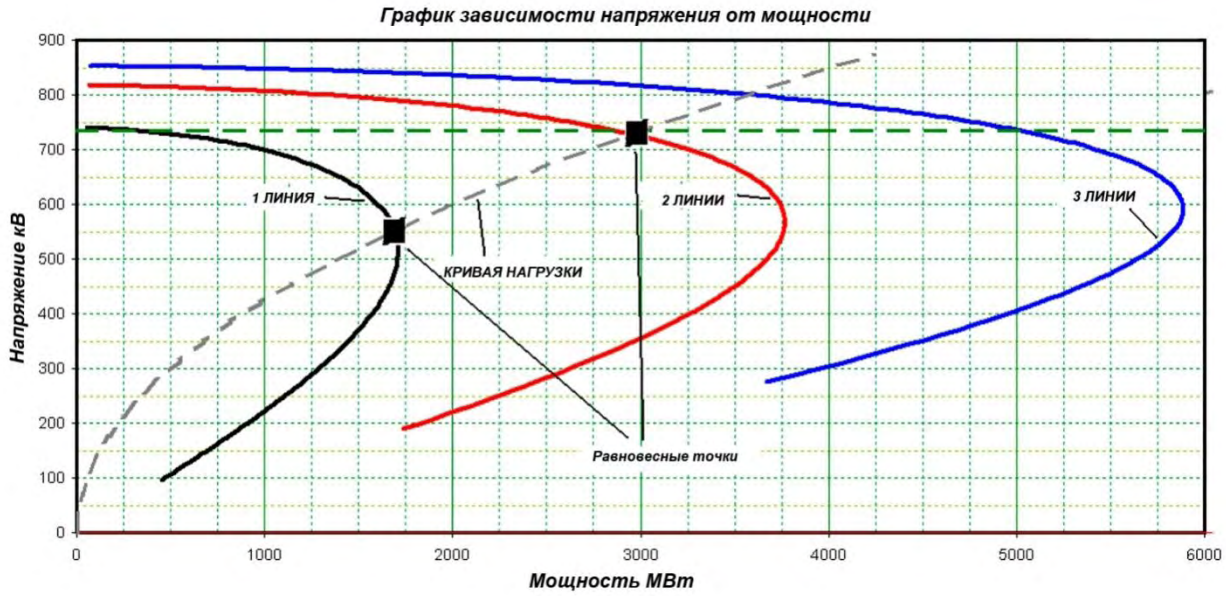



**Рисунок N-26 Равновесная точка на графике зависимости напряжения от мощности**

Этот пример показывает, что предприняли бы системы SIPS для восстановления устойчивости сети. Они анализируют топологию сети и при выявлении тяжелых режимов производят необходимые операции (отклонение нагрузки, генерации или комбинированные действия), чтобы сохранить устойчивость и функциональность электросети.

Теперь рассмотрим влияние на сеть в случае, если хакер возьмет под контроль релейную защиту линии и осуществит аварийное отключение силовых выключателей. Если электроэнергетическая система общего пользования не оборудована системами SIPS, скачок передаваемой мощности и напряжения может привести к потере устойчивого состояния сети, что, возможно, повлечет за собой обширное длительное нарушение энергоснабжения.

На рисунке 27 показано, как увеличение или уменьшение реактивной компенсации на линии электрической сети влияет на напряжение. Шунтирующие реакторы контролируют напряжение в линии электрической сети. При добавлении шунтирующих реакторов (МВАр) напряжение на линии понижается, а при их выключении – повышается. Серая линия – это кривая нагрузки; она пересекает кривые ЛЭП в точках равновесия сети (когда сеть устойчива). Черная линия изображает реактивную компенсацию трех ЛЭП при помощи добавления мощности 600 МВАр. Зеленая линия – это те же три линии без реактивной компенсации. Номинальное напряжение (735 кв) показано пунктирной зеленой линией. В этом примере мы рассматриваем нагрузку мощностью 5000 МВт на сеть 735 кВ. Для того, чтобы при поддержании номинального напряжения передать 5000 МВт, сохранив при этом устойчивость сети, мы должны добавить 600 МВАр реактивной компенсации. Если убрать всю реактивную компенсацию, напряжение повысится с 735 кВ до 810 кВ. Недокомпенсация приводит к повышению напряжения на нагрузке или в других точках сети.

Если хакер возьмет под контроль релейную защиту реактора и произведет аварийное отключение выключателей шунтирующего реактора, это приведет к перенапряжению, в результате которого электрооборудование может быть повреждено или уничтожено, а устойчивое состояние сети потеряно. В этом случае системы SIPS пошлют команду статическим и синхронным компенсаторам, расположенным на других участках сети, чтобы скорректировать напряжение до номинального уровня. В приложении С описываются примеры последствий успешной кибератаки на электрическую сеть.

В этом пункте представлены несколько примеров возможных проблем в случае, если хакер успешно захватит контроль над цифровой релейной защитой и выполнит операции, которые могут резко

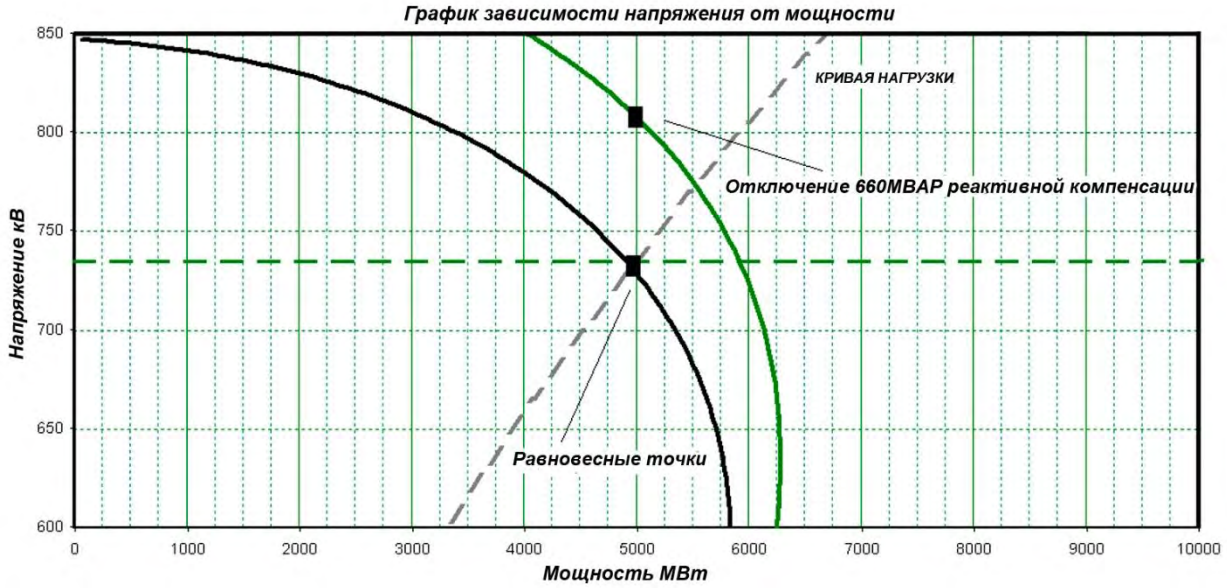



**Рисунок N-27 Влияние, вызванное потерей компенсации**

повлиять на устойчивость электрической сети. Нетрудно представить, насколько серьезным было бы проведение одновременных атак во многих точках сети. Несмотря на то, что в электроэнергетический системе общего пользования предусмотрено резервирование для предотвращения несрабатывания релейной защиты, это не помешает хакеру, который взял под контроль устройства релейной защиты, умышленно послать команду на аварийное отключение выключателя или изменить настройки защиты. И хотя хакерская атака на релейную защиту затронет только защиту оборудования, ее результатом может быть потеря устойчивости сети, создание эксплуатационных ограничений и изменение передаваемой мощности.

Когда электроэнергетическая система общего пользования оборудована системами SIPS, автоматизированная система обеспечивает устойчивость сети даже при разрушительных авариях. Даже если хакер через устройства релейной защиты попытался отключить линию или силовой трансформатор на подстанции, система SIPS выполнит действия для поддержания устойчивости и надежности сети. По этой причине такая система способствует защите от воздействий кибератак.

### N. 4 Угрозы системам SIPS

В предыдущем пункте обсуждались системы (ИЭУ или релейная защита), направленные на защиту специального оборудования. При возникновении неполадок релейная защита быстро отключает оборудование, для того чтобы избежать дополнительных повреждений оборудования и снизить риск потери устойчивости на участке электрической сети. Тем не менее, релейная защита сама по себе не является автоматизированной системой. Она может быть использована для обеспечения автоматизированной системы данными, но ее цель – защита не всей электросети, а конкретного электрооборудования.

Электрические сети должны быть способны выдерживать такие режимы, как потеря одной ЛЭП, потеря источников или снижение нагрузки в пределах запаса устойчивости. Когда происходят такого рода события, сеть должным образом их компенсирует, управляя уровнем напряжения, а системы регулирования электростанций в свою очередь управляют частотой и передачей мощности в электросети, для того чтобы сохранить устойчивую работу энергосистемы и минимизировать влияние на потребителей. Однако бывает так, что случаются нетиповые, более тяжелые происшествия, как например: потеря более двух параллельных линий, потеря подстанции или потеря источников или нагрузок, превышающая запас устойчивости. Все это может стать причиной серьезных сбоев. Когда происходят такие события, главной задачей является обеспечение безопасности сети и сохранение ее устойчивости, чтобы избежать длительного нарушения энергоснабжения. Крайне редко происходят аварии, оказывающие настолько разрушительное воздействие, что сохранить устойчивость сети уже невозможно и нарушения

энергоснабжения неизбежны. В таком случае основная цель уже заключается не в том, чтобы пытаться сохранить сеть в работе, а в том, чтобы спасти электрооборудование от перенапряжений, возникших в результате выхода сети из строя (обеспечить безопасность оборудования). Когда электрическая сеть отключается без серьезных повреждений, намного быстрее и проще ввести ее обратно в эксплуатацию.

Задачи систем SIPS заключаются в том, чтобы сохранять устойчивость сети, поддерживать непрерывность обслуживания потребителей и избегать серьезных повреждений электрооборудования в исключительных или экстремальных ситуациях. Существует множество типов систем SIPS, но цель этого пункта состоит не в представлении полного описания функциональных возможностей всех типов, а в том, чтобы обозначить воздействие на электрические сети кибератак, нацеленных на оборудование, формирующее системы SIPS. Рассмотрим один из типов таких схем, называющийся общесистемным. В [65] рассматриваются многие другие виды систем SIPS.

### N. 5 Общесистемные SIPS – наиболее сложные системы

На рисунке 28 приведена функциональная структура и пути обмена информацией между системами с широкой зоной контроля, защиты и управления. Они включают в себя системы устранения первичных неисправностей в работе основных и резервных систем защиты, а также SIPS, RAS, SPS, и глобальную систему контроля и наблюдения с синхрофазорами. К тому же, в центрах управления и терминалах технического обслуживания подстанции могут устанавливаться другие приборы и компьютеры, не указанные на рисунке, такие как концентратор векторных данных (синхрофазор), устройства оценки состояния и интерфейс оператора. При возникновении аварии в энергосистеме, для ее устранения используется основная релейная защита для систем высокого напряжения или основная релейная защита с двойным резервированием для магистральных электрических сетей сверхвысокого напряжения. Если из-за несрабатывания релейной защиты или сбоя в выключателях и т. д., неисправность не устраняется, срабатывает резервная релейная защита. Даже когда неисправность устранена, при тяжелых авариях или помехах в энергосистеме, таких как обрыв ЛЭП и разделение энергосистемы на части, в месте повреждения могут присутствовать неустойчивые или несбалансированные режимы, включая потерю устойчивости угла выбега ротора, отклонение частоты и напряжения от допустимых значений и прочие перегрузки. В таких случаях вступают в работу системы SIPS/RAS. Эта структура подразумевает глубокоэшелонированную защиту от неисправностей и аварий в электрической системе.

В целях стабилизации энергетической системы в течение допустимого времени, в системах с широкой зоной контроля, особенно в системах защиты от коротких замыканий, задаются жесткие требования относительно управления и надежности, эти требования соответственно применяются к релейной защите, ИЭУ, компьютерам управления и сетям связи. В таблице 12 представлены соответствующие требования к системам с широкой зоной контроля. Если система с широкой зоной контроля не отвечает этим требованиям, то она может не только работать неверно, но и ухудшать качество электроэнергии или даже прерывать электроснабжение.

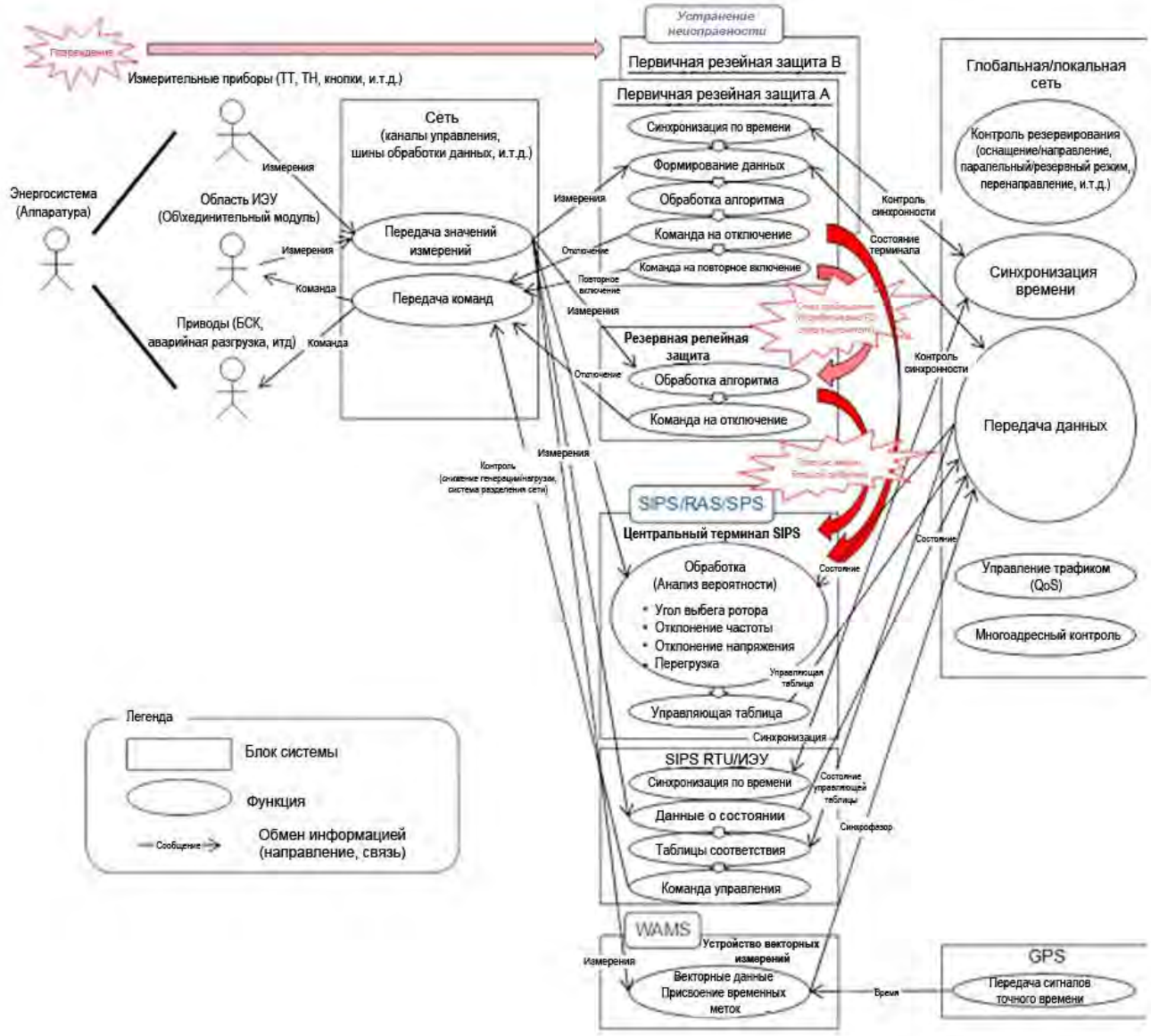



**Рисунок 28 Функциональная структура и пути обмена информацией систем с широкой зоной контроля**

**Таблица N-12 Эксплуатационные и коммуникационные требования к системам WAMPAC**

| | Основная РЗ[31] [32] [33] [34] [35] [36] | Резервная РЗ | Сравнение систем SIPS с 33 36 | | | | WAMS 35 38 |
|---|---|---|---|---|---|---|---|
| | | | Угол выбега ротора | Отклонение частоты | Отклонение напряжения | Перегруз-ка | |
| Надежность ПРИМЕЧАНИЕ 1 | $>1-10^{-5}$ | $> 1-(10^{-2}\div10^{-3})$ ПРИМЕЧАНИЕ 3 | Схожие значения с основной и резервной РЗ | | | | Не указано |
| Безопасность ПРИМЕЧАНИЕ 2 | $>1-10^{-6}$ | $> 1-(10^{-4}\div10^{-7})$ ПРИМЕЧАНИЕ 3 | Схожие значения с основной и резервной РЗ | | | | Не указано |
| Время срабатывания | < 33÷40 мс (< 2 cycles) | ~ 200 до 300 мс | 140÷500 мс | 200÷500мс | 500мс÷ 15с | От 400 мс до десятков | От секунд до минут |
| Задержка в линии связи | < 2.5÷10 мс | Не применяется для дистанционных защит | <10мс÷2с | <10÷110 мс | <25÷150мс | <30мс÷5с | < 1с |
| Разброс значений задержки в линии связи | < 100÷200 мкс (дифференциаль-ный ток) | | < 20 мс | < 20 мс | < 20 мс | < 1 с | N/A (Данные с привязкой ко времени) |
| Асимметричность значений задержки в линии связи | < 200÷400 мкс (дифференциаль-ный ток) | | Controlled routing required | | | | |
| Синхронизация времени | < 100÷200 мкс (дифференциаль-ный ток | | < 50 мкс | < 50 мкс | < 100 мс | < 1 с | < 1 мс (на основе GPS) |
| Степень ошибок связи | $< 10^{-6}\div10^{-8}$ | | $< 10^{-6}$ | | | | Не указано |
| Резервирование или несрабатывание системы связи | $< 10^{-7}$ для систем с двойным резервировани ем | | $< 10^{-7}$ и $3.1\cdot10^{-4}$ для систем с двойным и одиночным резервированием, соответственно | | | | Не указано |
| Время восстановления/пе реключения связи | < 50 мс | | < 50 мс | | | | Не указано |

[31] 57 ТК IEC "Оборудование телезащиты энергосистем – Выполнение и испытание – Часть 1: Командная система, "Международная Электротехническая комиссия IEC 60834-1, Издание 2.0, Октябрь 1999.

[32] 57 ТК IEC "Оборудование телезащиты энергосистем – Выполнение и испытание – Часть 2: Издание 1.0, Июнь 1993.

[33] РГ 10 ТК 57 IEC "Коммуникационные сети и системы для автоматизации энергосистем – Часть 90-1:

[34] СИГРЭ ОРГ D2B5.30 "Защиты линий и систем на основе цифровой автоматики и пакетной связи," СИГРЭ Техническая брошюра 521, 2012.

[35] IEC РГ 10 ТК 57 "Системы и сети связи на подстанциях – Часть 5: Требования к связи для моделей функционирования и устройства," Международная Электротехническая комиссия, IEC/TP 61850-5, Издание 2.0, Январь 2013.

[36] IEC РГ 10 ТК 57 "Системы и сети связи на подстанциях – Часть -90-12: Руководства по проектированию широкомасштабных сетей", Международная Электротехническая комиссия, IEC /TP 61850-90-12,в стадии разработки.

ПРИМЕЧАНИЕ 1 Допущение отсутствия отказов в срабатывании.

ПРИМЕЧАНИЕ 2 Допущение отсутствия нежелательных срабатываний (ложное аварийное отключение или нежелательное повторное включение)

ПРИМЕЧАНИЕ 3 Для удобства резервная защита и РЗ с блокировкой по каналам связи предполагаются одинаково надежными и безопасными.

Для рассмотрения вопроса информационной безопасности систем с широкой зоной контроля на рис. 28 стрелками и эллипсами показаны кибератаки, нацеленные соответственно на сбои обмена информацией и на функции оперативного управления. Основными к устранению являются указанные в таблице 12 кибератаки, ухудшающие требуемые характеристики и надежность. В таблице N-13 указаны некоторые кибератаки, нацеленные на снижение производительности и надежности, и их последствия.

Прежде не требовалась повышенная конфиденциальность информации. Для надежности и защищенности от незначительных кибератак, в системах с широкой зоной контроля и обмена информацией в настоящее время наиболее эффективны следующие контрмеры: резервная конфигурация и пути передачи информации, механизмы отслеживания ошибок цикла, проверка порядковых номеров элементов данных и механизм регулировки запаздывания. Вышеупомянутая глубокоэшелонированная структура защит систем с широкой зоной контроля также может справляться с некоторыми видами кибератак. Но даже применение контрмер не отменяет требований безопасности, особенно к задержкам в канале связи и времени срабатывания.

**Таблица N-13 Влияние кибератак на надежность и эксплуатационные требования, их последствия и контрмеры (примеры)**

| **Требования** | **Кибератака** | **Классификация ДЦК*** | **Последствия** | **Контрмеры** |
|---|---|---|---|---|
| Надежность (ИУЭ) | Атака типа "отказ в обслуживании" | A | Задержка устранения аварии или задержка в управлении, отказ аварийного отключения или управления | Резервные ИЭУ |
| Надежность (ИУЭ) | Атаки вмешательства, изменение ПО, внедрение вредоносного ПО) | A, I | Нежелательное аварийное отключение, отказ аварийного отключения или управления | Аутентификация пользователя, управление доступом на основе ролей, определение/сопротивление взлому |
| Задержка в линии связи | Задержка пакетов на изменение маршрута, внедрение конкурирующих пакетов | A | Задержка сигнала управления | Уплотнение портов, и упрочнение коммутаторы и маршрутизаторы, упрочнение кабелей с неметаллическим покрытием |
| Ошибки в синхронизации по времени | Подмена сообщений (Задержка и изменение пакетов управления методикой эксплуатационных испытаний) | I, A | Нежелательное аварийное отключение, отказ аварийного | Виртуальные локальные сети |

| Требования | Кибератака | Классификация ДЦК* | Последствия | Контрмеры |
|---|---|---|---|---|
| | Подмена данных GPS | | отключения из-за погрешности расчета, обусловленной ошибкой интервала дискретизации | Расположение антенны мониторинга (атака завершается неудачно, если злоумышленник знает точное расположение антенны).<br>Использовать несколько приемников для обнаружения данных о поддельном времени. |
| Ошибка связи | Изменение пакетов (Команд на отключение, управляющих таблиц), повторные атаки | I | Нежелательное аварийное отключение, отказ аварийного отключения или управления | Аутентификация сообщения |
| Конфиденциаль-ность информации | Похищение данных о конфигурации энергосистемы (центрального оборудования SIPS) | C | Включает повторные кибер и физические атаки | Шифрование |

* доступность, целостность и конфиденциальность

# Приложение О
# Детальное рассмотрение практических решений информационной безопасности

## О.1 Совместные усилия

Практические решения внедрения информационной безопасности требуют совместной работы инженеров по эксплуатации систем защиты и управления, сетевых инженеров и других профессионально квалифицированных сотрудников. Например, управление сетевыми устройствами (маршрутизатор, выключатели, система сетевой защиты и др.) обычно входит в обязанности сетевого инженера. Однако инженеры по эксплуатации систем защиты и управления должны работать совместно с сетевыми инженерами, чтобы удостовериться в том, что параметры конфигурации сетевых устройств не оказывают влияния на работу систем защиты и управления, их надежность и доступность.

## О.2 Физическая защита систем защиты и управления

Физическая защита включает множество различных аспектов, начиная от заблокированных ворот и дверей, дающих доступ к ИЭУ. Физические аспекты, такие как замки ворот и дверей, не рассматриваются в данной технической брошюре.

Физическая защита ИЭУ представляет собой ролевую модель управления доступом (РМУД), включающую пароль и уровни полномочий пользователя. Электроэнергетическая система общего пользования (ЭЭСОП) должна хранить базу данных разрешенных персоналу функций, доступ к которой для конкретного человека открывается паролем. Много различных аспектов ролевой модели управления доступом были обсуждены в технической брошюре СИГРЭ №427, опубликованной в августе 2010 года [66].

## О.3 Безопасность оконечного устройства систем защиты и управления

### О.3.1 Общие вопросы вредоносного ПО

Сложное вредоносное ПО быстро распространяется, особенно на оконечных устройствах, которые соединяют сети защиты и управления с незащищенными устройствами. Вирусы, такие как Stuxnet и Троянский конь, известный как Зевс, схожи тем, что создают пробелы в защите, они используют слабости безопасности оконечных устройств и уязвимости приложений, чтобы существенно поразить свои цели. То, чем они отличаются, – это метод передачи. По словам независимой исследовательской организации Ponemon Institute, респонденты их исследования назвали наиболее часто встречающимися сетевыми происшествиями атаки вредоносного ПО, атаки бот-сетей и внедрение SQL-кода. Самыми серьезными видами происшествий оказались атаки нулевого дня, внедрения SQL-кода и использование уязвимостей программного обеспечения, которому более трех месяцев. Респонденты больше всего обеспокоены действиями работающих в удаленном режиме сотрудников, загружающих неизвестные сторонние приложения и увеличивающих угрозу разрушительных атак вредоносного ПО, которые сложно обнаружить.

Согласно отчету о результатах исследования уязвимости данных компании-оператора сотовой связи Verizon в 2010 году, наиболее частым путем для атаки служат веб-приложения, сервисы и программное обеспечение удаленного доступа и контроля и путь обхода системы защиты канала управления.

### О.3.2 Появление эшелонирования безопасности оконечного устройства

Решением компании Lumension является переход к более целостному методу глубокоэшелонированной защиты. В центре размещается блок управления конфигурацией и внесением исправлений, а затем он окружается слоями управления приложениями, управления устройствами и антивирусом. Слои должны работать совместно, чтобы эффективно предотвратить риски безопасности пользователя, приложения и данных. Инженерам по эксплуатации систем защиты и контроля необходимо учитывать следующие способы и методы:

**Улучшить управление внесением исправлений:** Инженеры не могут просто включить Сервисы обновления серверов Window's (WSUS) и оставить управление внесением исправлений выполнять свои задачи. Уязвимости приложений защиты и управления встречаются во всё более распространяющихся сторонних (входят в комплект поставщика) средствах настройки, которым сервисы WSUS не помогут. Стандарт IEC 62443-2-3 предлагает улучшенный метод управления внесением исправлений, который следует рассмотреть.

**Задействовать антивирус:** Несмотря на то, что антивирус бесполезен по отношению к атакам нулевого дня, для защиты периметра сети защиты и управления он отлично блокирует известные угрозы.

**Вайтлистинг приложений защиты и управления:** Инженеры по эксплуатации защиты и управления должны тщательно изучить вайтлистинг приложений, который позволяет пользоваться только утвержденными приложениями и запрещает все остальные. По умолчанию вайтистинг защищает сеть защиты и управления без необходимости ожидания последнего патча уязвимостей или оценки антивируса. Он особенно важен для защиты от атак нулевого дня.

Инженеры по эксплуатации защиты и управления понимают управление внесением исправлений и круговую оборону антивируса. Они нуждаются в более глубоком понимании процедур управления вайтлистинга.

### O.3.3 Вайтлистинг приложений защиты и управления

Лучше всего начать с выхода за рамки использования антивируса – утверждает Эрик Орген при рассмотрении вопроса безопасности оконечных устройств. Главная идея Оргена – "Вайтлистинг приложений становится технологией безопасности, которая дает IT [инженерам по эксплуатации систем защиты и управления] настоящую возможность создания глубокоэшелонированной защиты, которая закроет все пробелы, существующие при использовании антивируса. Вайтлистинг устанавливает среду надежных приложений, которая предупреждает выполнение неизвестного или нежелательного ПО, в том числе сложные и неизвестные вредоносное программы."

Для защиты и контроля наиболее привлекательной особенностью вайтлистинга является возможность закрыть окно уязвимости без ложных срабатываний или неблагоприятных эффектов, влияющих на непрерывную (в режиме 24/7) работу систем защиты и управления. Вайтлистинг приложений не реагирует на уведомления об атаках – он рассматривает любые непредвиденные изменения в конфигурации оконечного устройства защиты и управления как атаку и блокирует изменение раньше, чем произойдет любое повреждение оборудования или сбой функционирования системы защиты и управления.

Однако, инженеры по эксплуатации систем защиты и управления могут персонализировать оконечные устройства защиты сети, чтобы защитить избранные области оконечного устройства. При правильном использовании пользователи могут запускать утвержденные приложения, не ослабляя контроль безопасности и эксплуатации. Например, безопасность оконечных устройств обеспечивает возможность ввода и вывода данных с помощью портативных устройств (например, персональных компьютеров) и других USB-устройств, таких как флеш-накопители и медиакарты, не вызывая нарушения безопасности.

## O.4 Контроль сетевой безопасности систем защиты и управления

Сетевая безопасность является важным структурным элементом для достижения многоуровневой защиты систем защиты и управления. Кроме того, она является неотъемлемой частью условной структуры (Рисунок 1). Она затрагивает аспекты связи основных случаев использования: автоматизация подстанции, автоматизация между двумя подстанциями, автоматизация между подстанцией и центром управления, а также удаленное проектирование.

В общем случае, сетевая безопасность выполняет следующие функции:

- Контроль доступа – основная составляющая контроля доступа заключается в том, чтобы иметь мощные механизмы идентификации для всех элементов системы защиты и контроля, подключенных к сети: пользователи, устройства и приложения. В общем

случае, только уполномоченный персонал, имеющий доступ к сети, и действующие устройства являются её частью.

- Конфиденциальность и целостность данных – целостность данных для всех операционных данных и данных систем защиты и управления является обязательным условием. Шифрование связи не является обязательным, за исключением случаев, в которых нормы требуют конфиденциальности данных.
- Обнаружение и снижение угрозы – цель состоит в том, чтобы защитить критически важные объекты от кибератак и внутренних угроз.
- Целостность устройств и платформ – защита устройств от угроз должна быть устойчива к кибератакам.

Кроме того, заложенные сетевые возможности обеспечивают широкий спектр функций для защиты связей между всеми компонентами системы защиты и управления. Ниже приведены наиболее важные функции:

- Методика качества обслуживания (КО) может помочь обнаружить нарушения потоков обмена информацией и представить решение по предотвращению отказов в обслуживании (ОО). В общем случае, КО обеспечивает следующие функции:
- Дополнительная выделенная полоса пропускания
- Уменьшение характеристик потерь
- Предотвращение и управление перегрузками сети
- Формирование сетевого трафика
- Установление приоритета трафика в сети

Внедрение КО в системы защиты и управления является важной мерой управления и защиты установки от различных вариаций атак, таких как внешние, внутренние, а также технические неисправности и неправильная настройка. Оно управляет источниками информации и упрощает использование нескольких типов трафика.

- Анализ сетевого трафика для оценки отклонений от нормы с целью обнаружения кибератак на систему защиты и управления.
- Управление производительностью контролирует и поддерживает производительность сети защиты и управления.
- Обнаружение и уведомление о неисправностях всех составляющих сети защиты и управления и ИЭУ защиты и управления, присоединенных к сети.
- С точки зрения сетевой структуры, топологии и аппаратного обеспечения, обязательными условиями являются следующие аспекты: правильный управляемый проект сети, используемый в соответствии с нагрузочным режимом, пропускной способностью и КО, а также правильный подбор и настройка маршрутизаторов и коммутаторов, включая резервирование.

Сетевая инфраструктура на основе технологии МКПМ (мультипротокольная коммутация по меткам) обеспечивает надежную и масштабируемую платформу для мультисервисных инженерных сетей, в которых защита и управление являются неотъемлемой составной частью. МКПМ и средства виртуализации повышают безопасность сети на основе следующих особенностей:

- Высокая степень доступности, резервирование и отказоустойчивость, задействованные в обновлении сервисного программного обеспечения, переключении с проверкой состояния и бесперебойном прохождении сигналов в сети
- Выявление, определение приоритета рисков и управление ими в процессе проектирования
- Сетевая надежность за счет локализации и изоляции критически важного трафика
- Передовые виды КО детального управления уровнем обслуживания

Генерирующие предприятия и организации по услугам передачи электроэнергии и мощности всё чаще работают над модернизацией и проектированием будущих энергосистем на основе приложений для умных сетей электроснабжения, требующих использования передовых систем телекоммуникации. В МКПМ предлагается проверенная платформа для взаимодействия многих пакетов использования приложений для передачи информации и сигналов управления через глобальную вычислительную сеть предприятия (ГВС). Конечно, в неё включаются и системы защиты и управления. Меры по переходу к технологии принимаются и дают возможность переосмыслить, модернизировать и усилить контроль безопасности. Масштабируемые структуры VPN обеспечивают безопасные и надежные решения для связи распределительных систем, таких как подстанции, между собой или связи подстанции и центра управления.

### О.4.1 Управление доступом

Управление сетевым доступом состоит из различных функций, которые могут объединяться в одном сетевом устройстве или одновременно применяться к одному оконечному устройству или приложению. Конечная цель состоит в том, чтобы гарантировать, что только авторизованные представители (устройства и персонал) имеют доступ к сети и подключенным к ней устройствам.

**Безопасность портов** наиболее важна для ограничения входного трафика на интерфейс коммутатора путем ограничения и определения MAC-адресов оконечных устройств, которым разрешен доступ к этому порту. Присваивая защищенные MAC-адреса[37] защищенному порту, порт не пересылает пакеты с адресами источников за пределы группы определенных адресов. Если достигается защищенный порт и максимальное число MAC-адресов или при попытке получить доступ к порту MAC-адрес станции отличается от любого из идентифицированных защищенных

MAC-портов, происходит нарушение защиты. Кроме того, если станция с защищенным MAC-адресом, настроенным или полученным на одном защищенном порте, пытается получить доступ к другому защищенному порту, происходит нарушение, о чем сообщает сигнал тревоги. В случае нарушения должна быть предусмотрена возможность настроить интерфейс на один из нескольких режимов нарушения (на основе ответного действия):

при пропускании пакетов с неизвестными адресами источников посылается SNMP-ловушка, регистрируется сообщение системного журнала и срабатывает счетчик нарушений; нарушение безопасности порта приводит к немедленному отключению интерфейса.

**Стандарт IEEE 802.1x (управление сетевым доступом с использованием портов)** определяет управление доступом на основе клиент-сервера и протокола аутентификации, который запрещает неавторизованным клиентам подключаться к локальной сети с помощью авторизованных (и должным образом аутентифицированных) доступных портов. Сервер аутентификации перед тем, как сделать доступными какие-либо возможности коммутатора или локальной сети, проверяет каждого подключенного к порту коммутатора клиента. До тех пор, пока клиент не прошел проверку, управление доступом по стандарту 802.1x разрешает информационный обмен только по расширяемому протоколу аутентификации (EAP) в локальной сети, протоколу канального уровня (LLDP) и протоколу основного дерева (Spanning Tree Protocol) через порт, к которому подключен клиент. После успешной аутентификации через порт может проходить обычный трафик. На Рисунке О-29 изображен алгоритм работы стандарта 802.1x при условии реализации внутри подстанции (технический клиент) с использованием сервера аутентификации, авторизации и учета (ААУ) в центре сетевого управления.

[37] Динамическое обучение или ручная конфигурация подвергают MAC-адреса опасности.


**Рисунок О-29 802.1x Контроль доступа**

**РМУД и ААУ** являются трудновыполнимыми из-за особенностей управления системой защиты. Средства управления безопасностью должны разрешать доступ к перечню команд и источников информации, доступных каждому пользователю посредством доменов и ролей при ограничении авторизации, когда пользователь должен иметь доступ к деятельности по управлению. Пользовательские роли определяют привилегии пользователей, такие как команды, которые пользователь может вводить, и действия, которые пользователь может осуществлять в определенной ситуации. Как правило, решение с использованием модели РМУД предлагает ряд заранее установленных ролей. Пользовательские роли содержат правила, которые определяют операции, разрешенные для осуществления пользователю, исполняющему роль. В каждой пользовательской роли может содержаться несколько правил, и каждый пользователь может иметь несколько ролей. Для реализации и настройки РМУД используется имя пользователя/комбинация паролей и/или идентификаторы по сертификату X.509. Сильные идентификаторы пользователей с РМУД дают гарантию, что только уполномоченный персонал связывается с подстанцией и элементами системы защиты и управления. Должны быть настроены формируемые многопользовательские группы с различными уровнями доступа к устройствам подстанции (таким, как ИЭУ). Протоколы RADIUS (Remote Authentication Dial In USER Service, служба удаленной аутентификации дозванивающихся пользователей) и TACACS+ (Terminal Access Controller Access Control System Plus, система управления доступом для контроллера доступа к терминалу) являются предпочтительными протоколами, предоставляющими ААУ пользователям и устройствам. Протокол TACACS+ представляет собой приложение системы безопасности, обеспечивающее централизованную аутентификацию пользователей, делающих запрос на получение доступа к устройствам сети. Сервисы TACACS+ централизованные, как правило, управляются из Центра Управления Сети. Цель TACACS+ заключается в обеспечении способа управления множеством точек доступа к сети из единой службы управления. Протокол RADIUS представляет собой распределенную клиент-серверную систему, которая обеспечивает защиту сети от несанкционированного доступа. Клиенты RADIUS функционируют на маршрутизаторах и коммутаторах. Клиенты отправляют запросы аутентификации в центральный сервер RADIUS, который содержит всю информацию об аутентификации пользователей и доступе к сетевым службам.

Фильтрация пакетов **списка управления доступом (СУД)** ограничивает сетевой трафик и использование сети для определенных пользователей и устройств. СУД обрабатывает трафик при его прохождении через маршрутизатор или коммутатор и разрешает или

запрещает прохождение пакетов через установленные интерфейсы или виртуальные локальные сети. СУД представляет собой последовательный набор условий разрешения и отказа, который применяется к пакетам. При получении пакета по интерфейсу коммутатор сравнивает поля в пакете со всеми приложенными СУД, чтобы убедиться, что пакет имеет необходимые разрешения для передачи пакета, исходя из критериев, указанных в списке доступа. Один за другим, он проверяет пакеты по условиям списка доступа.

### О.4.2 Конфиденциальность и целостность данных

С точки зрения систем защиты и управления целостность всех оперативных данных и данных защиты и управления имеет первостепенное значение. Конфиденциальность данных имеет большое значение в случаях, когда требования и нормы устанавливают шифрование связи. Целостность и конфиденциальность особенно важны при передаче данных между подстанциями или в случае удаленного доступа.

Основанная на протоколе IPSec гибкая и масштабируемая структура VPN (виртуальная частная сеть) шифрует все данные, передаваемые между сетями общего пользования или частными сетями подстанций. Сетевые VPN способны масштабировать и использовать возможности инфраструктуры открытого ключа (PKI) таких сетевых платформ, как, например, маршрутизаторы (на подстанции). Важнейшим проектным решением является расположение оконечных точек протокола IPSec. Оконечными точками оперирует доверенная сторона в защищенной зоне сети. Конфиденциальность и целостность данных, а также аутентификацию на подстанциях, подключенных посредством глобальной сети, обеспечивают решения VPN, такие как динамическая многоточечная виртуальная частная сеть (DMVPN) и виртуальная частная сеть передачи зашифрованной группы (GETVPN). В общем случае, механизмы шифрования канального и сетевого уровня сохраняют видимость данных на промежуточных узлах и разрешают использование основных сервисов IP, как КО (например, предотвращение ОО методами КО). Гибкие решения для защиты связей удаленного проектирования обеспечивают технологии VPN на основе протокола защиты транспортного уровня (TLS). Использование TLS-VPN (Web-VPN) позволяет сети подстанции безопасно расширяться за счет сотрудников по их ролям.

### О.4.3 Обнаружение и снижение угрозы

Для достижения цели защиты критически важных объектов систем защиты и управления от кибератак и внутренних угроз рассмотрим следующие измерения и средства:

**Сегментация сети** является эффективной мерой для разделения трафика в зависимости от классов приложения. В сети автоматизации подстанций виртуальные локальные сети делят трафик между сегментами (зоны безопасности, такие как Защита и управление, Проектирование и Многофункциональное обслуживание). Кроме этого, рекомендуется также делить трафик в пределах одного сегмента подстанции (например, для разделения данных векторных измерений и данных, полученных от ИЭУ). Также в целях разделения трафика по классам приложений следует использовать сегментацию глобальной сети; например, телемеханическая релейная защита, система КАС ДУ и проектирование. Строгую логическую сегментацию обеспечивает основанная на технологии МКПМ VPN виртуальная маршрутизация и переадресация (ВМП). В дополнение, дискретно применяются методы Качества обслуживания. Сегменты ВМП обычно в пределах подстанции имеют соответствующие виртуальные локальные сети, которые согласуют трафик сегмента беспроводных локальных сетей, реализованный на основе отображения один к одному с входящим/исходящим трафиком виртуальных локальных сетей.

**Устойчивая периметровая защита** является основой для концепции защиты зон с наличием системы сетевой защиты, как правило, в качестве функциональной возможности, предоставляемой маршрутизатором подстанции. Для разрешения передачи между зонами трафика используются подробно разработанные правила. Между зонами проходит трафик неявного отклонения только в случае, если правило пары зон разрешает прохождение специального трафика. Двумя примерами могут служить зоны защиты и управления на подстанции и в центре управления, соединенные между собой посредством глобальной сети. Используйте списки управления доступом для фильтрации, регистрации и авторизации

трафика, передаваемого между сегментами.

**Максимальная видимость** в сети является важной характеристикой качества, необходимой для поддержания контроля безопасности распознавания, который включает в себя все подключенные системы, устройства и события. Сетевые вторжения обнаруживаются с помощью систем предотвращения вторжений (СПВ) в критических точках сети подстанций. Как правило, СПВ является частью периметровой защиты, осуществляемой маршрутизатором подстанции или устройством СПВ. Блоки СПВ для обнаружения и предотвращения вредоносных программ могут быть обновлены при наличии ключей. Используя встроенный набор функций, СПВ предотвращает атаки в месте проникновения на подстанции и защищает маршрутизатор и сеть защиты и управления от ОО атак. Реагирование должно проходить в режиме реального времени посредством сигналов тревог и дальнейших действий. Ключевым требованием многих нормативных актов является регистрирование событий безопасности. Большое значение имеют журналы регистрации разных устройств с отметками по времени. Выделенный прибор для управления событиями системы защиты и регистрации аудита, как правило, диспетчер событий и информации о защите, предоставляет этот набор функций и располагается в центре управления сети. Кроме того, он предоставляет отчетность об аварийных событиях на основе соотношения регистрационных данных и сигналов тревоги для выявления нарушений безопасности (например, для контроля и установления соотношений периметровых и внутренних событий). Для защиты периметра безопасности подстанции от возможных атак отказа в обслуживании (ОО) обеспечивают ограничение уровня управления на всех выключателях и маршрутизаторе подстанции.

### О.4.4 Целостность устройств и платформ

Важнейшей задачей для устройств и платформ является необходимость удостовериться в том, что устройства не смогут попасть под угрозу и будут устойчивы к кибератакам. Чтобы отвечать требованиям, основными составляющими должны быть: устойчивая к взлому структура, образ микропрограммного обеспечения с цифровой подписью, заверенные NIST или эквивалентные алгоритмы шифрования информации, безопасное хранилище зашифрованных учетных данных и разработка кода безопасности. Для связи особой важности используйте устройства, такие как маршрутизатор и коммутаторы на подстанции, специализированное аппаратное, встроенное микропрограммное и программное обеспечение. Для этих целей также имеют большое значение конфигурационные аспекты. Для защиты локальной сети подстанции от взлома закройте (отключите) неиспользуемые порты всех коммутаторов локальной сети. Проверьте и включите порты, находящиеся в работе. Целостность устройств и платформ всех компонентов является необходимым условием обеспечения глубокоэшелонированной безопасности систем защиты и управления.

## О.5 Эксплуатационные ограничения

### О.5.1 Предоставление доверенного доступа к средствам защиты и управления

Необходимость ролевой модели управления доступом (РМУД) для защиты и управления четко и определенно изложена в технической брошюре 427[67] рабочей группы СИГРЭ B5.38. Вопросы управления схемами ролевой модели управления доступом защиты и управления этой группой не были рассмотрены. Внимание объединенной рабочей группы B5-D2.46 сосредоточено на наиболее сложном вопросе – объединенном управлении ролевой моделью управления доступом, необходимой для оперативной работы защиты и управления, которое включает несколько независимых организаций. Такими организациями являются фирмы-подрядчики и органы государственного регулирования, которым необходимо обеспечить доступ и управление использованием средств защиты и управления на законных основаниях. В некоторых ситуациях требуется доступ на сайт, в других – доступ из удаленных расположений. В любом случае, цель инженеров защиты и управления состоит в том, чтобы объявить тех, кто запрашивает доступ к средствам защиты и управления недоверенными. Для того, чтобы гарантировать доверенный доступ и использование этих средств, используют цифровые сертификаты с правами доступа для проверки и контроля, а также правами использования. Основной механизм осуществления РМУД в рамках жизненного цикла управления ключами описан в Приложении М.

### O.5.2 Централизованная ЭЭСОП правами РМУД

Одним из подходов является такой, когда ЭЭСОП управляет РМУД централизованно, запрашивая проверку всех цифровых сертификатов защиты и управления своим сервером РМУД. С учетом того, что требования к обеспечению своевременной поддержки технического обслуживания защиты и управления и разрешения проблем варьируются и носят временный характер, в централизованном подходе вводятся значительные временные задержки. Это делается для согласования и утверждения действий, чтобы должным образом проверить контроль доступа и использовать ограничения, указанные в цифровом сертификате пользователя.

- Период времени действия сертификата ограничивается в большинстве прав поддержки.
- Задавайте степень разрешения контроля использования: либо только права чтения, либо права чтения и написания. На изменение прав для всего персонала права имеют только избранные пользователи.

### O.5.3 Объединенное управление правами РМУД

Другой подход заключается в том, чтобы позволить всем субъектам, не входящим в ЭЭСОП, управлять созданием, проверкой и размещением своих собственных цифровых сертификатов. Этот подход переносит требование доверия с ЭЭСОП на проверяющую организацию субъекта, не входящего в систему. В этой ситуации вопросы централизованного управления являются более сложными, потому что все проверяющие организации должны согласовать их в установленные сроки.

### O.5.4 Общие рекомендации

Вопросы ролевой модели управления доступом к защите и управлению являются сложными и могут иметь самые разные схемы реализации, по рекомендациям объединенной рабочей группы B5-D2.46 необходимо ввести новую рабочую группу для решения этих вопросов.

## O.6 Максимальное использование компенсирующих механизмов безопасности

Инженеры защиты и управления называют три причины обеспечения компенсирующего контроля безопасности для защиты критически важных объектов и функций. Во-первых, традиционные системы, подсистемы и компоненты имеют недостаточные механизмы безопасности и должны прибегать к помощи систем периметровой защиты для осуществления функций защиты. Во-вторых, множество новых компонентов защиты и управления не обладают достаточным объемом памяти или вычислительных ресурсов для внедрения механизмов безопасности. В-третьих, время отклика защиты электроэнергетических систем не может допустить ни появление запаздывания связи, ни затрат времени обработки при выполнении сложных задач, таких как шифрование и дешифрование для защиты конфиденциальности и целостности данных при обмене информацией.

По этим причинам инженеры защиты и управления должны добиваться повышения первой линии защиты до максимума. В частности, контроль доступа локальной сети подстанции от интерфейсов, признанных "недоверенными". Вторая линия защиты состоит из нескольких механизмов безопасности, которые обеспечивают выполнение процессов пользовательского управления (например, права чтения/записи, указанные в цифровых сертификатах), сохранение ограниченного потока данных под управлением маршрутизаторов сети подстанции, а также управления сетевыми ресурсами, встроенными во все ИЭУ защиты и управления.

Основной задачей инженеров защиты и управления является обеспечение правильной настройки и обслуживания этих механизмов безопасности. Для осуществления этой задачи необходима совместная работа с ИТ-инженерами и независимыми экспертами по данным вопросам из персонала технической поддержки, работающего по контракту.

### O.6.1 Внесение исправлений в системы защиты и управления

Европейское агентство по сетевой и информационной безопасности (ЕАСИБ) предлагает качественные рекомендации по внесению исправлений в КАС ДУ для Европы [68]. В их докладе делается вывод о важности создания эффективной политики управления внесением исправлений организациями (ЭЭСОП). Данная техническая брошюра опирается на рекомендации ЕАСИБ, предлагая решения обеспечения информационной безопасности для систем защиты и управления, дополненные организационными указаниями и требованиями о соблюдении технического контроля.

### О.6.2 Введение ответственности разработчика за внесение исправлений в системы защиты и управления

Компоненты систем защиты и управления используют различные типы операционных систем (например, Windows, Linux и операционная система реального времени VxWorks) и сторонних приложений (например, базы данных, драйверы), имеющих хорошо известные уязвимости информационной безопасности, которыми пользуются для взлома.

Таким образом, разработчики защиты и управления должны обращать внимание на уязвимости информационной безопасности стороннего программного обеспечения, а также гарантировать, что их собственные разработки программного обеспечения функционируют "защищенно".

### О.6.3 Процесс управления уязвимостями разработчиком

На рисунке О-30 показан всеобщий процесс управления уязвимостями. Для своевременного решения проблем уязвимостей разработчики должны проводить четко регламентируемые исследования угроз информационной безопасности. Для этого исследования требуется актуальная информация о проблемах в области информационной безопасности, поступающая от различных поставщиков компонентов сторонних производителей (например, Microsoft, Sybase и другие), а также от организаций, как группа ГРКЧП (Группа реагирования на компьютерные чрезвычайные происшествия).

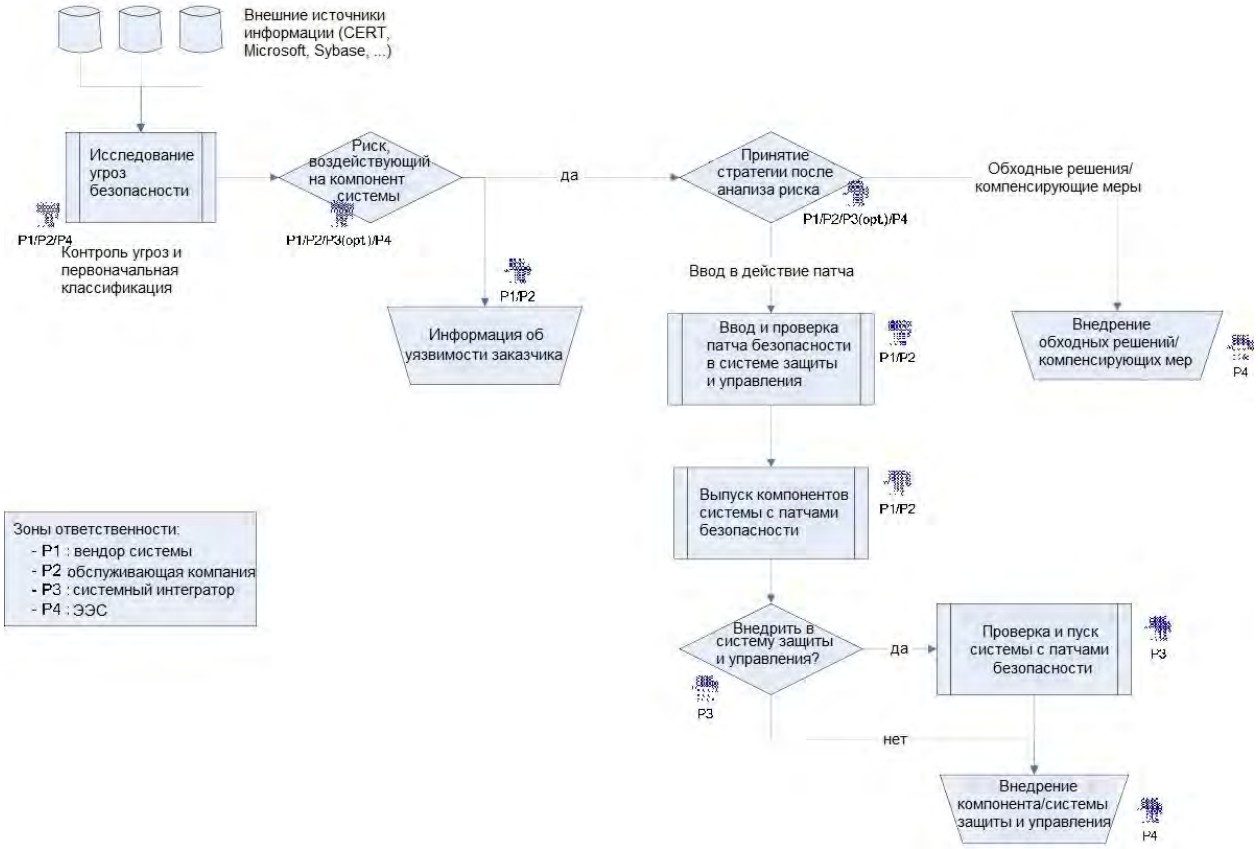



**Рисунок О-30 Процесс управления уязвимостями**

Для всех уязвимостей информационной безопасности необходима оценка для определения влияния на компоненты систем защиты и управления. Используется оценка каждой угрозы по шкале: не оценивается, низкий риск, средний риск, высокий риск и очень высокий риск. Кроме того, разработчик должен классифицировать влияние на оперативную работу. По этому первоначальному анализу формируется список уязвимостей информационной безопасности. Следующий этап включает объединение списка уязвимостей с анализом последствий, предоставленным в виде документа ЭЭСОП (заказчик). План-график доставки включается в комплект поставки заказчику при наличии возможности.

Имея представление о влиянии уязвимости на оперативную работу, временное решение или компенсирующие меры может определить сама ЭЭСОП[38] (или совместно с разработчиком) для уменьшения этого риска, пока разработчик не предоставит патчи безопасности.

### О.6.4 Поставка, контроль и проверка качества/верификация безопасности систем защиты и управления

Когда поставщик компонентов сторонних производителей выпускает патч безопасности, разработчик реализует его в своей системе. В этом случае сторонний производитель должен предоставить разработчику методику проведения теста, установки испытательного стенда, а также информацию о том, какие функции тестируются. Тогда у разработчика будут все необходимые данные для оценки точности результатов тестов.

Целью проверки патча безопасности в системе защиты и управления является не подтверждение того, что уязвимость системы безопасности устранена. Эту задачу выполняет поставщик компонентов сторонних производителей. Настоящая цель заключается в проверке того, что патч безопасности не оказывает влияния на функциональность системы защиты и управления и на надежность и эксплуатационные характеристики системы.

Как и для любой проверки системы, разработчик предоставляет список и результаты тестов, которые свидетельствуют об отсутствии влияния патча безопасности. В этом случае разработчик должен предоставить заказчику методику проведения теста, установки испытательного стенда, а также информацию о том, какие функции тестируются. Тогда у заказчика будут все необходимые данные для оценки точности результатов тестов.

Разработчик должен гарантировать, что внедрение патчей безопасности, а также свои собственные разработки происходят в безопасном режиме, то есть в процессе разработки не создаются угрозы информационной безопасности.

### О.6.5 Внедрение патчей систем защиты и управления

В зависимости от процесса управления конфигурацией разработчика (или процесса, определенного между электроэнергетической компанией и разработчиком) патчи безопасности поставляются с выпуском одного компонента или выпуском целой системы.

Поскольку выпуск патча безопасности согласуется с графиками технического обслуживания ЭЭСОП, разработчик и ЭЭСОП должны совместно определить политику проверок и поставок с учетом уровня важности рисков.
Нет смысла в выпуске новой версии системы при каждом появлении патча безопасности, так как часто могут быть огромные ограничения внедрения. Учитывая эти ограничения, более разумным представляется выпускать новую версию системы защиты и управления с частотой максимум два раза в год. Конечно, поставку можно произвести раньше в зависимости от уровня важности патча.
Внедрение патчей систем защиты и управления должно происходить по тем же правилам, которые установлены ЭЭСОП для внедрения функциональных обновлений или исправлений ошибок. Управление этими правилами регулируется внутренними процессами ЭЭСОП, которые не включены в данную техническую брошюру.

[38] ЭЭСОП также могут проводить свои собственные исследования угроз безопасности, чтобы иметь актуальные данные об уязвимостях даже при условии, что у них нет глубоких знаний об уязвимостях и потенциальном влиянии на системы и компоненты защиты и управления.

### О.6.6 Внедрение патчей системой ЭЭСОП

В некоторых странах регулирующие компании устанавливают определенные сроки для оценки и установки патча безопасности. Например, в стандартах защиты объектов жизнеобеспечения Североамериканской корпорации по обеспечению надежности электроэнергетических систем (NERC CIPS):

NERC-CIP-007-3-R3.1 требует оценки в течение 30 календарных дней.
NERC-CIP-007-5-R2.2 требует оценки в течение 35 календарных дней.
NERC-CIP-007-5-R2.3 распространяется на патчи, установленные в R2.2; и требует в течение 35 календарных дней после завершения оценки выполнить одно из следующих действий: применить установленные патчи, создать датированный план мер по ликвидации последствий,

# Приложение P
# Расширение рекомендаций США по укреплению защиты информационной безопасности

## P.1 Отчет Комитета советников при Президенте США по вопросам науки и техники (PCAST)

В этой брошюре выводы и рекомендации PCAST [США] адаптированы к сфере систем защиты и управления. Отчет PCAST [69] кратко изложен в одном основном и шести дополнительных пронумерованных выводах. Расширенный набор применимых к защите информационной безопасности систем защиты и управления выводов приведен ниже.

## P.2 Основной вывод

За счет совокупности статических предупредительных мер по обеспечению безопасности, которые будут приняты государственными регулирующими организациями и ЭЭСОП, информационная безопасность не будет достигнута. Скорее, ей требуется набор процессов, которые непрерывно передают информацию о развивающейся угрозе, чтобы осуществить меры защитного реагирования. В данной технической брошюре описаны подобные процессы с акцентом на интеграцию для выполнения традиционных задач, решаемых инженерами сети и защиты и управления.

Вывод 1: Федеральное правительство США (и правительства других стран) редко следуют рекомендациям. По этой причине ЭЭСОП не могут следовать примерам, осуществляемым правительственными организациями; они должны устанавливать собственные примеры и активизировать усилия, чтобы сделать более сложным проведение регулярных кибератак путем внедрения рекомендаций для систем защиты и управления. Для создания механизмов защиты информационной безопасности в продуктах и сервисах ЭЭСОП им необходимо включать специальные требования к информационной безопасности в своих спецификациях снабжения для поставщиков защиты и управления. При таких механизмах защиты ЭЭСОП должны тщательно обеспечивать, контролировать и поддерживать настройки и параметры в них.

Вывод 2: Многие ЭЭСОП подпадают под ту или иную форму федерального или местного (на уровне штата) регулирования. Во многих случаях есть возможность (в полной мере согласующаяся с целями существующего законодательства) для продвижения и достижения рекомендованных методов информационной безопасности защиты и управления. В частности, регулирующий орган должен запрашивать не конкретный перечень мер информационной безопасности, а процесс принятия и дальнейшего улучшения рекомендаций информационной безопасности. С этим подходом хорошо согласуются описанные в этой технической брошюре стандарт IEC 62443, Подсектор электроэнергетики – Модель зрелости возможностей информационной безопасности (ES-C2M2) и Указания форума Jericho Forum.

Вывод 3: Процессы непрерывного совершенствования, проводимые ЭЭСОП, но проверяемые сторонней компанией, с большей вероятностью создадут эффективную культуру информационной безопасности в организациях защиты и управления, чем санкционированные государством статические списки мер безопасности. Техническая брошюра поддерживается в этом выводе; в нем предлагаются специальные показатели информационной безопасности защиты и управления, которые используются для проверки эффективности управления информационной безопасностью.

Вывод 4: Для улучшения способности реагировать в режиме реального времени происходит более широкий обмен данными угроз среди ЭЭСОП – в соответствующих условиях и по общепринятым интерфейсам – между ЭЭСОП и правительством. В разделе 6.1.2 описаны методы реагирования инженеров защиты на неисправности, вызванные кибератаками, и необходимость эффективного использования общих данных в отчетах о происшествии.

Вывод 5: Поставщики интернет-услуг должны способствовать развитию сферы информационной безопасности путем действий в реальном времени. Эта услуга может облегчить распространение данных о происшествиях, описанное в разделе 6.1.2.

Вывод 6: В будущем создание структур защиты и управления нужно будет начинать с того, что каждая составляющая системы защиты и управления должна быть предназначена для работы в неблагоприятной обстановке. Обществу необходимо больше исследований для стимулирования систем с динамическими защитами в реальном времени для дополнения утвержденных подходов. В сфере защиты и управления в данной технической брошюре поддерживается этот вывод. Особое внимание уделяется безопасности периметровой защиты и компенсирующим мерам безопасности.

**Словарь терминологический**

| | |
|---|---|
| MAC-адреса | MAC addresses |
| MPLS (мультипротокольная коммутация по меткам) | MPLS (multiprotocol label switching) |
| SNMP-ловушка | SNMP trap |
| аварийное отключение | trip |
| автоматизация подстанции | substation automation |
| анализ последствий | impact analysis |
| атаки бот-сетей | botnet attacks |
| аутентификация пользователей | user validation |
| база данных системы планирования и контроля энергопотребления. | EMS data |
| безопасность оконечного устройства | endpoint security |
| белый список | whitelisting |
| бесперебойное прохождение сигналов в сети | nonstop forwarding |
| беспроводные локальные сети | WLAN |
| вводный (ознакомительный) курс, начальная подготовка | awareness training |
| веб-приложения | web applications |
| вендор | vendor |
| виртуальная локальная сеть | VLAN |
| виртуальная маршрутизация и переадресация | virtual routing and forwarding |
| внедрение SQL-кода | SQL injections |
| внесение исправлений | patching |
| вредоносное ПО | malware |
| вспомогательная выделенная полоса пропускания | supporting dedicated bandwidth |
| вторичная защита | secondary protection |
| выключатель | switch |
| генерирующие предприятия | utilities |
| глобальная сеть | WAN |
| глубокоэшелонированная защита | defence-in-depth |

| | |
|---|---|
| глубокоэшелонированная безопасность | security-in-depth |
| группа реагирования на компьютерные чрезвычайные происшествия (группа CERT) | CERT (Computer Emergency Response Team) |
| детальное рассмотрение | deep dive |
| динамическая устойчивость | transient stability |
| длительное нарушение энергоснабжения сети | blackout |
| должностная обязанность | job responsibility |
| доступ к сетевым службам | network-service access |
| жизненный цикл управления ключами | key management life cycle |
| заблокированные ворота | locked gates |
| запланированные мероприятия | scheduled intervention |
| запрос аутентификации | authentication request |
| инженер по эксплуатации систем защиты и управления | P&C engineer |
| интеллектуальное электронное устройство (ИЭУ) | intelligent electronic device (IED) |
| информационная безопасность | cybersecurity |
| информационная защита | cyberdefence |
| информационные атаки | cyber-initiated intrusions |
| инцидент, аварийное происшествие | incident |
| исследование | survey process |
| исходные параметры системы защиты и управления | P&C metrics |
| ИТ-инженеры | IT engineers |
| КАС ДУ (Комплексная автоматизированная система диспетчерского управления) | SCADA (Supervisory Control and Data Acquisition) |
| качество обслуживания(QoS) | quality of services (QoS) |
| кибератака | cyber-initiated attack |
| Комитет советников при Президенте США по вопросам науки и техники (PCAST) | [U.S.] President's council of advisors on science and technology (PCAST) |
| компания Lumension | Lumension |
| конструкционный блок | building block |

| | |
|---|---|
| контроль безопасности и эксплуатации | security and operation controls |
| контроль сетевой безопасности | network security control |
| корректировка, исправление | patch |
| критически важные объекты (КВО) | critical assets |
| ликвидировать последствия | recover from |
| ложные срабатывания | false positives |
| локальная сеть | LAN |
| маршрутизатор | router |
| мероприятия | initiatives |
| место проникновения | entry point |
| метод обеспечения | assurance method |
| метод передачи | delivery method |
| механизм безопасности | security mechanism |
| механизмы отслеживания ошибок цикла | frame error detection mechanisms |
| многопользовательский | multiple user |
| многофункциональное обслуживание | multiservice |
| нарушения потоков обмена информацией | traffic abnormalities |
| Национальный институт стандартов и технологии США | NIST |
| неблагоприятная обстановка | hostile environment |
| несанкционированный доступ | intrusion |
| несрабатывание | miss-operation |
| нормы и мероприятия в области безопасности | security policies and procedures |
| нормы и мероприятия в области информационной безопасности | cybersecurity policies and procedures |
| обеспечивать хакеру условия | provide a hacker an easy environment |
| обладать быстродействием | act quickly |
| обнаружение и снижение угрозы | threat detection and mitigation |
| обслуживающий персонал | utility personnel |
| общесистемный | System Wide |

| | |
|---|---|
| Объединенное управление | Federated management |
| ограничение плоскости управления | control plane policing |
| операционная готовность | availability (of P&C systems) |
| организация по услугам передачи электроэнергии и мощности | TSO (transmission service organization) |
| ответное действие | response action |
| отказ срабатывания | miss tripping |
| отказы в обслуживании (DoS) | denial-of-service (DoS) |
| отражаться на | impact |
| отчет о результатах исследования уязвимости данных | Data Breach Investigations Report |
| отчет об оценке ситуации | situation assessment report |
| оценочный лист | scorecard |
| параметры конфигурации | configuration settings |
| патчи безопасности | security patches |
| переключение с проверкой состояния | stateful switchover |
| периметровая защита | perimeter security |
| план действий | response plan |
| план действий, план реагирования на происшествия | incident response plan |
| план-график доставки | delivery roadmap |
| ПЛК (программируемый логический контроллер) | PLC (programmable logic controller) |
| подготовка по вопросам инцидентов в системе информационной безопасности | cybersecurity incident training |
| подсектор электроэнергетики – модель зрелости возможностей информационной безопасности (ES-C2M2) | Electricity Subsector - Cybersecurity Capability Maturity Model (ES-C2M2) |
| подстанционное оборудование защиты и управления | substation P&C equipment |
| пользовательские роли | user roles |
| помещение главного щита управления | control building |
| правила допустимого использования сети | acceptable use policies |
| предпочитаемый, приоритетный | preferred |

| | |
|---|---|
| препятствие | roadblock |
| привилегии пользователей | user privileges |
| приложение системы безопасности | security application |
| применение, использование, внедрение | deployment |
| приоритет трафика в сети | traffic priorities across the network |
| профессиональная квалификация | specialized skills |
| путь обхода системы защиты | backdoor |
| равное разделение | even split |
| распределенная клиент-серверная система | distributed client/server system |
| распределительные системы | distributed systems |
| расширяемый протокол аутентификации (EAP) | Extensible Authentication Protocol (EAP) |
| регистрация аудита | audit logging |
| резервирование | redundancy |
| резервирующие системы защит | redundant protection systems |
| резервные защиты и УРОВ (устройство резервирования отказов выключателей). | backup protection and breaker failure protection |
| рекомендации | best practices |
| релейная защита и управление | P&C (protection and control) |
| ролевая модель управления доступом (RBAC) | role-based access control (RBAC) |
| руководящие принципы (указания) | guidelines |
| самонастраиваемая защита (на генераторы и силовые трансформаторы, реагирует на ток нагрузки) | adaptive protection |
| санкционированный государством | government-mandated |
| сбой | fault |
| сервер архивных данных | historian |
| сервисы обновления серверов Window's (WSUS) | Window’s Server Update Services (WSUS) |
| сетевой инженер | network engineer |
| сетевые вторжения | network intrusions |
| сетевые устройства | network devices |

| | |
|---|---|
| силовой выключатель | line breaker |
| система управления паролями | password management system |
| система компенсации, состоящая из последовательно включенных конденсаторных батарей | serial capacitors bank compensation systems |
| система сетевой защиты | firewall |
| система управления доступом для контроллера доступа к терминалу (TACACS+) | TACACS+ (Terminal Access Controller Access Control System Plus) |
| системы защиты и управления | P&C systems |
| системы предотвращения вторжений (IPS) | intrusion prevention systems, IPS |
| служба удаленной аутентификации дозванивающихся пользователей (RADIUS ) | RADIUS (Remote Authentication Dial In USER Service) |
| служба управления | management service |
| служебные руководящие указания | utility guidelines |
| событие системы защиты | security event |
| совместные усилия | collaboration efforts |
| список управления доступом | Access Control List (ACL) |
| средства настройки | configuration tools |
| средства управления безопасностью | security management tools |
| стандарты защиты объектов жизнеобеспечения Североамериканской корпорации по обеспечению надежности электроэнергетических систем | NERC CIPS |
| сторонние приложения | third-part apps |
| существующее наделяющее полномочиями законодательство | existing enabling legislation |
| существующие пробелы в защите | actual security breaches |
| схемы защиты целостности системы | SIPS |
| телемеханическая релейная защита | Tele-Protection |
| тестовая (оценочная) программа, сравнительный анализ | benchmark |
| технический персонал | field technicians |
| техническое обслуживание | maintenance |
| традиционные системы | legacy systems |

| | |
|---|---|
| трафик неявного отклонения | implicit deny traffic |
| требования и нормы | requirements and regulations |
| требования нормативных документов | regulatory requirements |
| тяжелый режим | severe event |
| удаленное проектирование | remote engineering |
| удаленный доступ | remote access |
| указания форума Jericho Forum | the Jericho Forum commandments |
| умные сети электроснабжения | smart grid |
| управление использованием | use control |
| управление конфигурацией и внесением исправлений | patch and configuration management |
| управление производительностью | performance management |
| управление системой защиты | security administration |
| уровень важности рисков | risk criticality |
| уровни полномочий пользователя | user permission levels |
| условная структура | notional architecture |
| устойчивость электрической сети | stability of the electric network |
| утвержденные подходы | hardening approaches |
| ухудшение экономической ситуации | economic downturn |
| уязвимость | vulnerability |
| физическая защита | physical security |
| фильтрация пакетов | packet filtering |
| центр сертификации | certificate authority |
| Центр Управления Сети | Network Control Centre |
| человеко-машинный интерфейс | human-machine interface |
| шифрование связи | encryption of communication |
| шлюз безопасности | security gateway |
| эксплуатационные ограничения | operational constraints |
| эксплуатационные характеристики системы | system performances |
| Электроэнергетическая система общего | electric power utility (EPU) |

| | |
|---|---|
| пользования (EPU), энергетическая компания | |
| элемент сети связи | communication network component |
| явление наведения эдс | inductive effects |
| явно выраженные правила | explicit rule |