



А. И. Белоус

# КИБЕРБЕЗОПАСНОСТЬ ОБЪЕКТОВ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА

Концепции, методы и средства обеспечения



## Оглавление

Предисловие .....	3
Введение .....	11
<b>ГЛАВА 1. ОСОБЕННОСТИ АВТОМАТИЗАЦИИ ОБЪЕКТОВ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА .....</b>	<b>22</b>
1.1. Цифровизация и автоматизация промышленности: направления, проблемы и риски.....	22
1.2. Структура топливно-энергетического комплекса .....	28
1.3. Цифровые технологии, как неизбежный этап эволюции предприятий ТЭК.....	33
1.4. Общая характеристика средств автоматизации объектов нефтегазовой отрасли .....	39
1.4.1. Ретроспективный анализ ситуации в области средств автоматизации объектов нефтегазовой промышленности.....	39
1.4.2. Особенности обеспечения кибербезопасности нефтегазовых компаний.....	47
1.4.2.1. Объекты и системы управления нефтегазовой отрасли .....	47
1.4.2.2. Информационная безопасность нефтегазовых компаний.....	52
1.4.3. Основные технические характеристики контроллеров и программно-технических комплексов.....	56
1.4.4. Характеристика каналов ввода/вывода контроллеров .....	60
1.4.5. Коммуникационные возможности контроллеров .....	65
1.4.6. Новые технологии в производстве контроллеров.....	83
1.4.7. Программное обеспечение.....	84
1.4.7.1. Программное обеспечение станций операторов/диспетчеров .....	86
1.4.8. Автоматизированные системы управления компрессорных станций.....	88
1.4.8.1. Автоматизированное рабочее место диспетчера компрессорной станции (АРМД КС).....	96
1.4.9. Уязвимости систем диспетчерского управления предприятий нефтегазового комплекса .....	97
1.4.9.1. Общая характеристика систем диспетчерского управления .....	97
1.4.9.2. Основные функции АСДУ для нефтегазового комплекса .....	101

1.5. Основные особенности обеспечения кибербезопасности на объектах ТЭК.....	103
1.6. Краткий ретроспективный анализ наиболее известных киберинцидентов.....	106
<b>ГЛАВА 2. КИБЕРОРУЖИЕ – КЛАССИФИКАЦИЯ, СРЕДСТВА И МЕТОДЫ ПРИМЕНЕНИЯ.....</b>	<b>121</b>
2.1. Введение в проблему .....	122
2.2. Определение и классификация информационного оружия .....	126
2.3. Определение и классификация кибервоздействий .....	135
2.4. Наиболее распространенные средства кибервоздействий.....	145
2.4.1. Удаленные сетевые атаки.....	145
2.4.2. Примеры реализации кибервоздействий с использованием метода удаленных сетевых атак .....	150
2.5. А кто это сделал? Проблемы идентификации исполнителей кибератак.....	152
2.5.1. Техническая прелюдия.....	152
2.5.2. Зачем нужна идентификация источника кибератаки .....	155
2.5.3. Технические сложности решения задачи идентификации источника кибератаки .....	158
2.5.4. Определение источников кибератак .....	160
2.6. Человеческий фактор как основная угроза кибербезопасности объектов ТЭК.....	164
<b>ГЛАВА 3. КИБЕРБЕЗОПАСНОСТЬ ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ ИНФРАСТРУКТУР.....</b>	<b>174</b>
3.1. Тенденции развития и особенности цифровизации промышленных инфраструктур.....	174
3.1.1. Особенности цифрового управления промышленными инфраструктурами.....	174
3.1.2. Основные угрозы безопасности цифрового производства .....	177
3.1.3. Эволюция парадигмы информационной безопасности производства .....	182
3.1.4. Подходы к обеспечению кибербезопасности цифрового производства.....	183
3.2. Физические угрозы электроэнергетических инфраструктур.....	189
3.3. Обобщенная структура управления энергосистемой .....	190
3.4. Основные уязвимости промышленных информационно-коммуникационных систем.....	192

3.5. Оценка рисков безопасности в энергетических системах .....	199
3.5.1. Киберугрозы и промышленные информационно-коммуникационные технологии.....	199
3.5.2. Сбор и обработка информации.....	202
3.5.3. Оценка рисков .....	202
3.5.4. Принятие решений и реализация действий .....	203
3.6. Типовые сценарии процесса анализа рисков для электроэнергетической системы.....	203
3.6.1. Сбор и обработка информации.....	203
3.6.2. Оценка рисков в электроэнергетической отрасли .....	206
3.7. Стандарты и методы обеспечения кибербезопасности электроэнергетических инфраструктур .....	217
3.7.1. Стандарты безопасности – общие критерии и подходы.....	217
3.7.2. Стандарты американского общества приборостроителей (ISA) .....	224
3.7.3. Стандарты международной организации по стандартизации (ISO).....	225
3.7.4. Стандарты национального института стандартов и технологий (NIST).....	228
3.7.4.1. Специальные публикации NIST 800 .....	228
3.7.4.2. Руководство по обеспечению безопасности промышленных систем управления (ICS) (NIST 800-82).....	229
3.7.4.3. Руководство по управлению рисками для ИТ-систем (NIST 800-30) .....	230
3.7.4.4. Руководство по обработке инцидентов в сфере компьютерной безопасности (NIST 800-61).....	232
3.7.5. Стандарты Североамериканской корпорации \ по надежности электроснабжения (NERC).....	234
3.7.6. Подходы к обеспечению национальной безопасности в США .....	239
3.7.6.1. DHS – Национальная стратегия по защите киберпространства .....	239
3.7.6.2. Центр по анализу угроз и рисков для инфраструктуры национальной безопасности DHS (HITRAC) .....	240
3.7.6.3. Особенности оценки кибер угроз в энергетическом секторе США .....	244
3.7.6.4. Защитные программы Министерства национальной безопасности США (DHS).....	246

3.7.6.5. InfraGard ФБР .....	247
3.7.6.6. Межведомственное сотрудничество, направленное на обеспечение информационной безопасности.....	247
3.7.6.7. Правоохранительные органы онлайн (LEO).....	248
3.7.6.8. Региональные системы обмена информацией (RISS).....	248
3.7.6.9. Система обмена информацией о национальной безопасности (HSIN).....	249
3.7.7. Подходы к обеспечению кибербезопасности в Англии .....	249
3.7.8. Концептуальные подходы к обеспечению кибербезопасности в Нидерландах.....	256
3.7.8.1. Национальный консультативный центр по критическим инфраструктурам (NAVI) .....	256
3.7.8.2. Стратегия национальной безопасности Нидерландов .....	258
3.7.8.3. Руководство по методике оценки национальных рисков (NRA) .....	260
3.8. Программно-аппаратные решения компании Моха по обеспечению промышленной кибербезопасности.....	265
<b>ГЛАВА 4. ОСНОВЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ЦИФРОВЫХ ЭЛЕКТРОПОДСТАНЦИЙ .....</b>	<b>281</b>
4.1. Сравнение цифровых и традиционных электрических подстанций по критериям надежности и живучести.....	281
4.1.1. Основные особенности цифровых электрических подстанций .....	281
4.1.2. Сравнительный анализ надежности и живучести традиционных и цифровых подстанций.....	283
4.2. Кибербезопасность цифровых подстанций.....	286
4.2.1. Государственная политика в области кибербезопасности в электроэнергетической отрасли.....	286
4.2.2. Основные направления повышения кибербезопасности цифровых подстанций.....	289
4.3. Основные технические требования к проектированию кибербезопасных цифровых электроподстанций .....	291
4.3.1. Особенности организации передачи данных в системах на базе МЭК-61850.....	291
4.3.2. Особенности проектирования кибербезопасных цифровых электроподстанций.....	293

4.4. Особенности обеспечения кибербезопасности релейной защиты цифровых электрических подстанций .....	300
4.4.1. Введение в проблему .....	300
4.4.2. Основные известные уязвимости релейной защиты .....	303
4.4.3. Возможные пути устранения основных уязвимостей релейной защиты .....	306
4.4.4. Аппаратный метод обеспечения релейной защиты от преднамеренных дистанционных деструктивных воздействий .....	307
4.5. Цифровая электрическая подстанция на основе аппаратно-программной платформы «Эльбрус» .....	311
4.5.1. Аппаратно-программная платформа «Эльбрус» как основа ЦПС в киберзащищенном исполнении .....	311
4.5.2. Технические характеристики и возможности программно-аппаратной платформы «Эльбрус» .....	313
ГЛАВА 5. КИБЕРБЕЗОПАСНОСТЬ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ .....	318
5.1. Особенности автоматизированных систем управления технологическими процессами атомной электростанции .....	318
5.1.1. Особенности оборудования и технологических процессов на атомной электростанции .....	318
5.1.2. Технологические системы АЭС .....	320
5.1.3. Основные функции асу ТП АЭС .....	327
5.1.4. Типовая структура и состав АСУ ТП АЭС .....	330
5.2. Особенности организации информационной защиты атомных электростанций .....	345
5.2.1. Уровни информационной защиты атомных станций .....	345
5.2.2. Особенности концепции безопасности белорусской АЭС .....	350
5.3. Основные киберугрозы для атомных электростанций и пути их нейтрализации .....	362
5.3.1. Кибератаки на электроэнергетические объекты – реальные угрозы .....	362
5.3.2. Основные пути нейтрализации киберугроз для атомных электростанций .....	367
5.3.2.1. Общее понятие о кибербезопасности АЭС .....	367
5.3.2.2. Уровни обеспечения кибербезопасности АЭС .....	368
5.3.2.3. Организационно-технические меры обеспечения кибербезопасности АЭС .....	369

5.3.2.4. Минимальный состав критических сведений об АЭС, подлежащих специальной защите.....	371
5.3.2.5. Опасность периодов замены оборудования и регламентных процедур .....	372
5.3.2.6. Анализ живучести как фактор повышения кибербезопасности .....	373
5.3.2.7. Новая роль аудита безопасности компьютерных систем АЭС .....	375
5.4. Обеспечение кибербезопасности электроэнергетической системы США.....	377
5.5. Кибероперация «Олимпийские игры», как пример подготовки и реализации гибридной кибератаки на объекты ядерной энергетики.....	384
5.5.1. Особенности обеспечения кибербезопасности в Исламской Республике Иран.....	384
5.5.2. Особенности контрразведывательной деятельности в области обеспечения безопасности ядерных объектов.....	392
5.5.3. Техническое обоснование выбора ключевого объекта кибератаки.....	397
5.5.4. Кибероперация «Олимпийские игры» .....	402
5.5.5. Особенности применения вируса Stuxnet как разновидности кибероружия.....	405
5.6. Авария на Саяно-Шушенской ГЭС – техногенная катастрофа или кибердиверсия? .....	408
5.6.1. Официальная версия катастрофы .....	408
5.6.2. Последствия аварии .....	411
5.6.3. Мнения независимых экспертов .....	413
5.6.4. Техничко-экономические характеристики гидроэнергетического комплекса.....	414
5.6.5. Возникновение аварийной ситуации.....	416
5.6.6. Расследование причин аварии .....	418
5.6.7. Причины аварии .....	418
5.6.8. Динамика процесса развития аварии .....	421
5.6.9. Критика официальной версии причин аварии .....	423
5.6.10. Последствия аварии .....	426
<b>ГЛАВА 6. ДОВЕРЕННАЯ ЭКБ КАК ОСНОВА «ПИРАМИДЫ КИБЕРБЕЗОПАСНОСТИ» В ЭЛЕКТОРОЭНЕРГЕТИКЕ .....</b>	<b>436</b>
6.1. Изменение структуры классической «пирамиды производственной безопасности» .....	436

6.2. Основы проектирования кибербезопасной электронной аппаратуры для объектов ТЭК.....	443
6.2.1. Введение в проблему.....	443
6.2.2. Поучительные эпизоды из авторской биографии связанные с исследованием «троянской темы» .....	453
6.2.3. Оценка безопасности этапов стандартного маршрута проектирования микросхем .....	464
6.2.4. Потенциальные агенты (организаторы) атак с использованием аппаратных троянов в микросхемах .....	470
6.2.5. Авторская попытка систематизации имеющихся знаний о методах обеспечения безопасности каналов поставки микросхем для отечественных электроэнергетических инфраструктур .....	472
6.3. Классификация аппаратных троянов в микросхемах ответственного назначения .....	475
6.3.1. Постановка задачи .....	475
6.3.2. Основная классификация аппаратных троянов в микросхемах ответственного назначения.....	477
6.4. Методология проектирования кибербезопасных микросхем для электронных систем управления объектами ТЭК.....	484
6.4.1. Постановка задачи .....	484
6.4.2. Анализ типового маршрута проектирования микросхем .....	487
6.4.3. Возможные типы кибератак .....	489
6.4.4. Основные различия между разработкой безопасных микросхем и разработкой безопасных программ .....	491
6.4.5. Особенности обеспечения жизненного цикла разработки безопасного программного обеспечения.....	492
6.4.6. Методы безопасного проектирования микросхем для ответственных применений .....	494
6.4.6.1. Этапы безопасного проектирования микросхем .....	494
6.4.6.2. Описание моделей угроз.....	495
6.4.6.3. Прослеживаемость в микросхеме.....	496
6.4.6.4. Цикл обнаружения .....	498
6.4.7. Экспериментальные результаты применения метода HTDS.....	500
6.4.8. Краткий обзор близких по тематике HTDS исследований .....	504
6.5. Современные технологии контроля безопасности в микроэлектронике .....	506

6.5.1. Введение в проблему.....	506
6.5.2. Эволюция классической парадигмы проектирования микросхем ответственного назначения .....	508
6.5.3. Место и роль технологий контроля безопасности в современной микроэлектронике .....	510
6.6. Основные алгоритмы (пути) внедрения троянских микросхем в технические объекты вероятного противника .....	515
6.7. Состояние и перспективы решения проблемы импортозамещения ЭКБ в отечественной нефтегазовой отрасли.....	521
6.8. Особенности взаимодействия Министерства энергетики и Министерства обороны США в сфере обеспечения кибербезопасности электроэнергетических структур .....	533
6.8.1. История создания и основные функции Министерства энергетики США.....	533
6.8.2. Стратегия Министерства обороны США по обеспечению безопасности ЭКБ .....	541
6.8.2.1. Основные положения стратегии безопасности.....	541
6.8.2.2. Политика Министерства обороны США в области планирования и реализации методов защиты каналов поставок микросхем военного назначения .....	547
6.8.2.3. Основные требования МО США к доверенным источникам приобретения изделий микроэлектроники.....	554
6.8.2.4. Нормативная база Министерства обороны США по обеспечению безопасности каналов поставки микросхем.....	555
6.8.2.4.1. Введение в проблему .....	558
6.8.2.4.2. Описание структуры типового плана программной защиты.....	561
6.8.2.4.3. Краткое описание структуры нормативного документа.....	563
6.9. Сравнительный анализ принципов и форм обеспечения защиты секретной информации в министерствах обороны и энергетики США .....	577
6.9.1. общие принципы построения системы защиты секретной информации.....	577
6.9.2. Особенности организации процедуры допуска к секретной информации руководителей организаций – подрядчиков .....	580
6.9.3. Особенности проведения процедуры собеседования с руководителями подрядчиков.....	581

6.9.4. Процедура оформления допуска персонала к секретным документам .....	583
6.9.5. Срок действия допуска к секретной работе.....	584
6.9.6. Особенности организации процедур проверок (аудитов) подрядчиков .....	585
6.9.7. Особенности обучения правилам обеспечения режима секретности.....	587
6.9.8. Классификационное руководство CG-SS-3 .....	588
6.9.9. Особенности процедуры организации допуска на секретный объект .....	589
6.9.10. Как и где обеспечивается доступ к секретной информации (специальные зоны).....	591
Приложение 1 .....	606
Приложение 2 .....	619