Confidential

RUSSIA

The circulation of this report has been strictly limited to the members of the *Trialogue* Club International and of the Centre russe d'études politiques.

This issue is for your personal use only.

Published monthly in Russian and in English by *Trialogue Company Ltd.*

Issue № 12 (240), vol.15. 2016

27 декабря 2016 г.

Олег Демидов сообщает из Москвы:

КИБЕРПРЕСТУПНОСТЬ *У ПОРОГА* ГРАЖДАНСКИХ ЯДЕРНЫХ ОБЪЕКТОВ:

РОССИЙСКИЙ ВЗГЛЯД НА ПУТИ НЕЙТРАЛИЗАЦИИ УГРОЗЫ

АННОТАЦИЯ

Вызовы в сфере кибербезопасности стали одной из ключевых проблем для операторов объектов критической инфраструктуры (КИ) по всему миру, причем киберинциденты более не обусловлены лишь случайными сбоями или человеческим фактором, как это было ранее. Фокус угрозы сместился на умышленные кибератаки, совершаемые опытными акторами, которые руководствуются криминальными или политическими мотивами.

При этом общемировые тенденции технологического развития делают КИ объективно более уязвимыми для кибератак. Критические инфраструктуры все теснее связаны между собой – эта неизбежная тенденция диктуется необходимостью оптимизации бизнес-процессов. Однако обратной стороной медали становится открытие «парадного входа» в системы КИ для киберпреступников.

Особенно яркой иллюстрацией этих тенденций среди всех критически важных отраслей являются гражданские ядерные объекты (ГЯО), которые стали мишенью номер один для продвинутых акторов в киберпространстве, – считает консультант ПИР-Центра Олег Демидов, эксперт в области кибербезопасности.

В этом выпуске Russia Confidential эксперт поясняет причины особой уязвимости ГЯО к киберугрозам и определяет пути их нейтрализации, опираясь на аналитические наработки ПИР-Центра, – одного из ведущих российских «мозговых центров», проводящего исследования в данной области.

ГРАЖДАНСКИЕ ЯДЕРНЫЕ ОБЪЕКТЫ ПОД КИБЕРУГРОЗОЙ, ИЛИ *ДЖИНН НА СВОБОДЕ*

Гражданские ядерные установки стали мишенью для целенаправленных кибернетических воздействий уже в целом ряде стран. Наиболее известны инцидент на американской АЭС Дэвис-Бессе, сеть которой в 2003 г. поразил компьютерный червь; кибероперация *Олимпийские игры*, проводившаяся в 2005-2012 гг. против мирной ядерной инфраструктуры Ирана с использованием вируса *Stuxnet* и другого передового вредоносного ПО (см. схему 1); кибершпионаж против южнокорейского оператора АЭС KHNP в декабре 2014 г. и заражение сети АЭС Гундреммингген в Германии в апреле 2016 г. Судя по всему, этот список будет продолжен, принимая во внимание выводы, проистекающие из этих инцидентов:

- ***Потенциальный объем ущерба для объектов, на которые нацелены кибератаки, резко возрос. Передовые образцы вредоносного ПО нацелены непосредственно на устройства в промышленных сетях и предназначены для проведения полномасштабных операций киберсаботажа. Яркий пример – Stuxnet.***
- ***Однократное выявление и расследование инцидента не гарантирует устранения угрозы, так как инструменты, используемые для атаки, могут быть легко модифицированы и использованы повторно.***
- ***Векторы угроз выходят за рамки привычных и включают в себя атаки на третьих лиц, социальную инженерию и другие нетрадиционные технологии.***

Говоря попросту, опасный *джинн* на сегодня оказался *выпущенным из бутылки*.

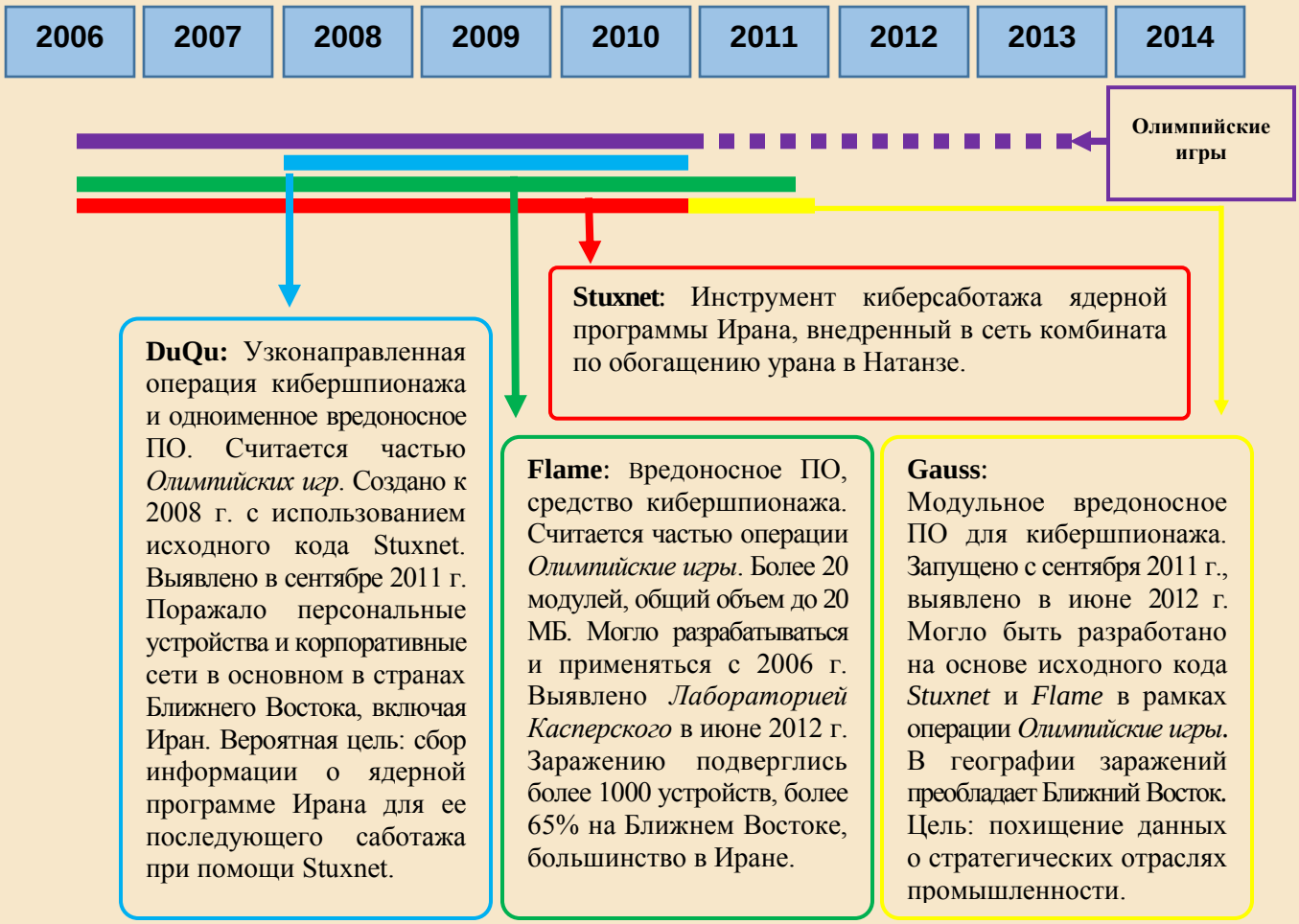

Схема 1: Хронология операции *Олимпийские игры*

Специфику развития инфраструктуры ИТ в секторе мирной ядерной энергетики также определяют некоторые **тенденции в сфере технологии:**

- Во-первых, подключение онлайн выходит за рамки корпоративных и офисных сегментов сетей АЭС и обогатительных установок. Автоматизированные системы, обеспечивающие выполнение критически важных технологических процессов на ядерных объектах, также основаны на цифровых технологиях и подключены к Интернету. Другой подключенный к сети сегмент включает в себя датчики и сенсоры, установленные на промышленном оборудовании для мониторинга его работы и отправки данных для систем мониторинга параметров функционирования. Какими бы *умными* и эффективными ни были эти системы и устройства, они становятся слишком многочисленны, что затрудняет обеспечение их безопасного взаимодействия.

- Во-вторых, корпоративные и офисные сегменты сетей ядерных объектов повсеместно подключены к Интернету для удобства обмена данными с внешними подрядчиками, консультантами и т.д.

- В-третьих, эти тенденции сопровождаются *мобильной революцией*, растущим рынком удаленных онлайн-услуг для систем управления промышленными процессами через Интернет с мобильного устройства (*SCADA в кармане*). Эти новшества расширяют периметр сетей, подлежащий защите, и создают новые потенциальные векторы атаки для злоумышленников.

Хотя эти тенденции развития характерны для всех секторов КИ, гражданские ядерные объекты стоят особняком. Каждая АЭС имеет сотни автоматизированных систем управления технологическими процессами (АСУ ТП) и десятки тысяч датчиков и сенсоров, что ведет к следующим неизбежным последствиям:

- ***Инфраструктурная сложность ядерных объектов ограничивает возможность применения накопленного опыта и лучших практик с точки зрения обеспечения кибербезопасности.***
- ***Огромное количество критически важных ИТ-компонентов делает операторов гражданских ядерных объектов зависимыми от слишком большого числа поставщиков; в результате, становится крайне сложно обеспечить целостность цепочек поставок.***
- ***Стандартные подходы к обеспечению кибербезопасности здесь оказываются недостаточны. Требуются дополнительные стратегии, такие как кибербезопасность на этапе проектирования, мониторинг сетевого трафика в режиме реального времени, внедрение криптографии в промышленные сети. Подобные меры не внедряются одномоментно, нужны масштабные долгосрочные инвестиции и широкая дискуссия о регуляторных мерах.***

ПРИНИМАЯ ВЫЗОВ: УСИЛИЯ ГОСУДАРСТВ И МИРОВОГО СООБЩЕСТВА

На **национальном уровне** правительства предпринимают ряд усилий для смягчения киберугроз ГЯО, однако эти меры явно не поспевают за эволюцией угроз.

- В большинстве государств кибербезопасность ГЯО лишь начинает оформляться в качестве отдельного предмета регулирования на общенациональном уровне. К основным проблемам относится нечеткое распределение регуляторных функций между государственными органами, а также зазоры и дублирование регуляторных функций. Во многих развивающихся странах такие функции бессистемно разбросаны между множеством регуляторов, которые недостаточно плотно взаимодействуют друг с другом.

- Еще одна проблема – отсутствие профильного для данного сектора регулятора, что обуславливает слабую обратную связь от представителей частного сектора. Кроме того, негибкость концепции физической ядерной безопасности (ФЯБ) иногда

препятствует разработке гибридного регуляторного подхода, который бы охватывал специфические вопросы сектора гражданской ядерной инфраструктуры. К этому зачастую добавляется нехватка интеграции международных рекомендаций, руководств и лучших практик в регуляторные нормы по обеспечению кибербезопасности ГЯО на национальном уровне.

На **международном уровне** дискуссия о кибербезопасности ГЯО протекает в условиях нормативного вакуума и отсутствия механизмов совместного реагирования и расследования киберинцидентов. В виду чувствительности данной сферы, кибератаки против ГЯО не подпадают под действие международных механизмов противодействия и предотвращения компьютерных преступлений, таких как Конвенция по борьбе с компьютерной преступностью Совета Европы от 2001 г. Тем не менее, открытым остается окно возможностей, связанное с деятельностью **Группы правительственных экспертов ООН**, хотя Группа предлагает государствам лишь добровольные, юридически не обязывающие нормы, которые к тому же рассматривают ГЯО не отдельно, а в совокупности с другими объектами КИ.

Наконец, в части технических руководств, тренингов, наращивания потенциала и повышения осведомленности о компьютерной безопасности ключевую роль играет **МАГАТЭ**.

И все-таки, 90% работы ожидает впереди. Прежде чем принять необходимые нормы, мировые лидеры должны, как минимум, разработать универсальную таксономию в отношении киберугроз гражданским ядерным объектам.

Обнадеживает то, что внимание на задачу предотвращения киберугроз ядерным объектам все чаще обращает **ООН**. В июле 2016 г. был опубликован Доклад Генерального секретаря по итогам работы Консультативного совета по вопросам разоружения. В документе Совет сопоставил масштабы потенциальной угрозы использования террористами киберсредств с тем чтобы вызвать человеческие жертвы, разрушение и нарушение функционирования инфраструктуры, с последствиями применения химического, биологического и радиологического оружия, и предложил Генеральному секретарю вынести этот вопрос на рассмотрение в рамках предстоящих международных форумов.

ВКЛАД РОССИЙСКИХ *МОЗГОВЫХ ЦЕНТРОВ*: НАРАБОТКИ ПИР-ЦЕНТРА

Помимо представителей промышленности, правительств и международных институтов, значительные усилия на анализ проблемы и выявление путей ее решения направляются экспертным сообществом. Одна из таких попыток была предпринята ведущей российской неправительственной научно-исследовательской организацией – **ПИР-Центром**.

- Весной 2016 г. ПИР-Центр опубликовал доклад *«Кибербезопасность гражданских ядерных объектов: оценка угрозы и определение дальнейших шагов»*, подготовленный по итогам консультаций с ведущими отраслевыми экспертами в Москве и Женеве. Исследование предлагает базовую модель классификации киберугроз в отношении ядерной инфраструктуры (см. схему 2 на следующей странице) и трехуровневое видение будущих шагов, а именно: для отрасли, национальных регуляторов и международных площадок.

На **техническом уровне** необходимо внедрение новых подходов к обеспечению кибербезопасности ГЯО, прежде всего за счет взаимодействия операторов таких объектов с ИТ-поставщиками. Необходимо свести к минимуму риски скрытого функционала в критически важных ИТ-компонентах за счет более интенсивного тестирования на проникновение (пентеста), нечеткого тестирования (фаззинга) и глубокого сканирования прошивок программно-конфигурируемых устройств нижнего уровня. Позитивную роль может сыграть и более тесный обмен опытом и лучшими практиками между ведущими ИТ-поставщиками и операторами ГЯО. Значимой составляющей нового подхода может стать обеспечение кибербезопасности на этапе проектирования объектов и внедрение современных средств криптографии в

промышленные сети. В случае с АЭС, поставщикам устройств на объекте имеет смысл делиться с операторами исходными кодами своей продукции.

На **регуляторном уровне** приоритетной целью является более полная интеграция кибербезопасности ГЯО в концепцию ФЯБ, что позволит устранить функциональные бреши и дублирование функций между регуляторами, отвечающими за кибербезопасность и ядерную безопасность. Для этого необходим интенсивный национальный диалог между регуляторами, должное внимание со стороны государственных органов и принятие комплексного законодательства, рассматривающего кибербезопасность ГЯО в качестве отдельного предмета. При этом МАГАТЭ, накапливая лучшие практики передовых стран, может предоставлять развивающимся странам эталонные модели подходов. Перед госорганами и операторами ГЯО также стоит задача вырастить поколение специалистов с новым профессиональным видением, отличным от традиционного подхода к обеспечению ФЯБ, но при этом способным дополнить и обогатить его. Достижению этого могут способствовать инновации в системе высшего образования и поддержка тренингов, семинаров и диалоговых форматов с участием представителей как сектора ядерной энергетики, так и ИТ-отрасли.

На **международном уровне** в рамках формата ГПЭ ООН возможно разрешение вопросов таксономии, понятийного аппарата и классификации секторов КИ и кибератак против них. Встречи пятого созыва Группы в 2017 г. могли бы стать вкладом в достижение общего видения по данной проблеме, если новый доклад ГПЭ напрямую затронет вопросы киберзащиты ГЯО и будет содержать предложения о добровольных нормах. Наконец, некоторые из более ранних предложений ГП могли бы быть доработаны с прицелом конкретно на сектор ГЯО. Примером может служить норма об обеспечении целостности цепочек поставок для критически важных ИТ-систем.

Хотя полностью отправить *джинна* киберугроз назад в бутылку малореалистично, согласованные усилия на указанных трех уровнях могут помочь значительно ослабить эту угрозу для мировой ядерной энергетики.

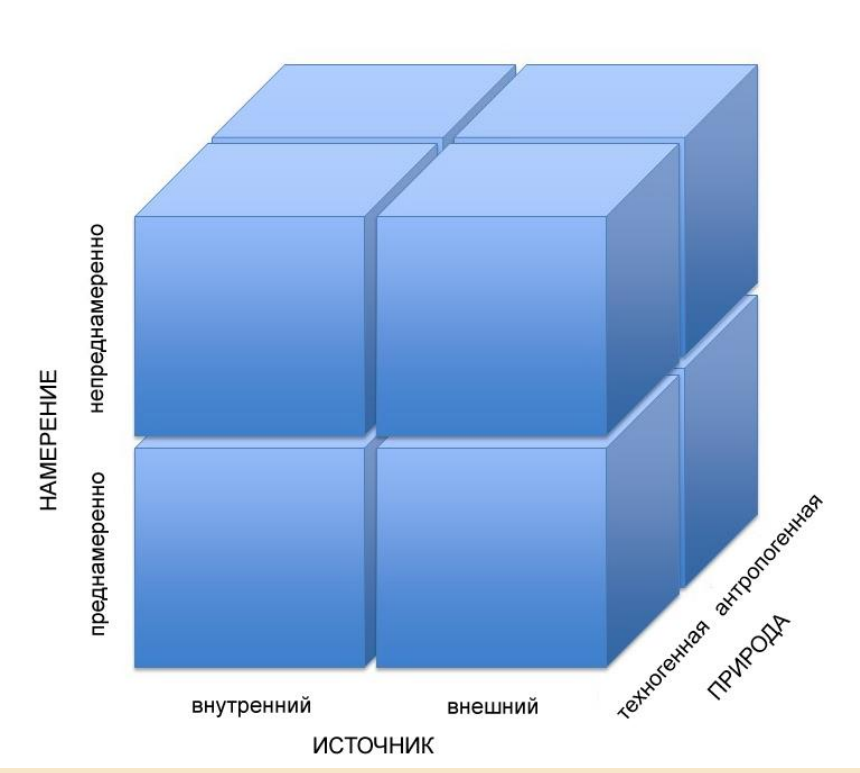

Схема 2. Базовая модель классификации киберугроз ГЯО.
Источник: ПИР-Центр

Автор статьи – Олег Демидов, консультант ПИР-Центра, эксперт по кибербезопасности.

Редактор: Юлия Фетисова

Москва-Женева, Декабрь 2016 г.

Выдержки из документа «Международный Клуб Триалог. Условия и правила членства».

3. Права членов Клуба

3.1. Индивидуальные члены Клуба имеют право:
3.1.3. Получать 1 экземпляр бюллетеня эксклюзивной аналитики Russia Confidential по электронной почте, на выбранном языке (русском или английском). По правилам Клуба, передача бюллетеня третьим лицам не допускается.[…]
3.2. Корпоративные члены Клуба имеют право:
3.2.3. Получать 2 экземпляра бюллетеня эксклюзивной аналитики Russia Confidential по электронной почте, на выбранном языке (русском или английском) либо на обоих языках одновременно, передавать этот бюллетень другим представителям корпоративного члена Клуба. По правилам Клуба, передача бюллетеня третьим лицам, не являющимся членами Клуба, не допускается.[…]

4. Обязанности членов Клуба

4.1. Все срочные члены Клуба обязаны:
4.1.6. Не передавать полученные материалы бюллетеня Russia Confidential, а также пароли доступа на сайт Клуба физическим и юридическим лицам, не являющимся членами Клуба. […]

6. Russia Confidential

6.1. Бюллетень эксклюзивной аналитики Russia Confidential выпускается ООО «Триалог» исключительно для личного пользования членов Клуба.
6.2. Бюллетень содержит сжатую эксклюзивную аналитику по вопросам международной безопасности, внешней и внутренней политики России и государств СНГ, подготовленную ведущими экспертами специально для Russia Confidential.
6.3. В течение не менее 30 дней со дня выхода материалы бюллетеня являются конфиденциальными и не могут цитироваться и передаваться лицам, не являющимся членами Клуба.
6.4. По прошествии не менее чем 30 дней ООО «Триалог» может снять эксклюзивный и конфиденциальный статус с материала, после чего в этих случаях он может быть опубликован в других изданиях и может быть использован для цитирования членами Клуба.
6.5. Бюллетень распространяется по электронным адресам членов Клуба 1 раз в месяц по русском или английском языке, по выбору члена Клуба.
6.6. По запросу члена Клуба, он может также получить бумажную версию бюллетеня на выбранном им языке.

Уважаемые члены Международного клуба Триалог,

завершается сезон-2016 работы Клуба, и мы рады **пригласить Вас продлить членство в Международном клубе *Триалог* на 2017 год или на 2017 - 2018 годы**.

В 2017 г. члены Клуба продолжат получать от нас эксклюзивную информацию по вопросам, связанным с приоритетами внешней политики Российской Федерации, а также современными вызовами и угрозами международной безопасности. На 2017 г. запланировано проведение **5 заседаний Международного клуба *Триалог***, 4 из которых пройдут в Москве, а 1 за рубежом. Члены клуба получат серию статей журнала *Индекс Безопасности в электронном виде*, **12 номеров** бюллетеня эксклюзивной аналитики *Russia Confidential* (на русском или английском языке), наши электронные информационные и аналитические рассылки.

Как и прежде, специалисты Международного клуба *Триалог* и партнерской организации ПИР-Центра открыты к обмену мнениями по ключевым международным проблемам.

Членство в клубе с 2017 г.

При оплате **до 30 декабря 2016 г.** размер ежегодного членского взноса составит:

Период	Индивидуальное	Корпоративное
01.01.17 – 31.12.17 (1 год)	45 000 руб.	72 000 руб.
01.01.17 – 31.12.18 (2 года)	81 000 руб.	126 000 руб.

При оплате **до 31 января 2017 г.** размер ежегодного членского взноса составит:

Период	Индивидуальное	Корпоративное
01.01.17 – 31.12.17 (1 год)	50 000 руб.	80 000 руб.
01.01.17 – 31.12.18 (2 года)	90 000 руб.	140 000 руб.

Напоминаем Вам, что в рамках **корпоративного** членства действует **схема «1+1»**, когда в работе Клуба участвуют **два представителя** одной организации.

По всем вопросам, связанным с членством в Международном клубе *Триалог*, следует обращаться по электронной почте secretary@trialogue-club.ru или по тел.: +7 (985) 764-98-96.

С уважением,

Председатель,
Международный клуб *Триалог* **Д.В. Поликанов**