КИБЕРБЕЗОПАСНОСТЬ ОБЪЕКТОВ ЭЛЕКТРОЭНЕРГЕТИКИ: ВЧЕРА, СЕГОДНЯ, ЗАВТРА

Cybersecurity of power facilities: past, present and future

According to ICS-CERT 295 incidents of cybersecurity breach have been reported in the USA critical infrastructure in 2015. Moreover, the second place – 46 cases – covers the energy sector. Such aggregated information on the incidents on critical infrastructure facilities of Russia, unfortunately, is missing. At least in the public access.

По данным ICS-CERT, за 2015 год было зарегистрировано 295 инцидентов нарушения кибербезопасности на объектах критической инфраструктуры США. Причем второе место – 46 случаев – занимает сектор энергетики. Подобная агрегированная информация по инцидентам на объектах критической инфраструктуры России пока, к сожалению, отсутствует. По крайней мере, в открытом доступе.

Дмитрий ЯРУШЕВСКИЙ,
руководитель отдела кибербезопасности АСУ ТП АО «ДиалогНаука»

Dmitry YARUSHEVSKY,
Head of IACS Cyber Security Department of DialogNauka, JSC

ДиалогНаука

О ТОМ, ЧТО УЖЕ БЫЛО

Тем не менее самые громкие события не остаются незамеченными. Менее чем за год в энергетической отрасли произошло несколько действительно значимых и заметных инцидентов, связанных с кибератаками. Во-первых, нельзя не упомянуть об атаках на Украинскую энергосеть с использованием вредоносного ПО Black Energy.

В декабре 2015 года осуществлен ряд успешных атак, в ходе которых предположительно были изменены конфигурации RTU (программно-аппаратные устройства среднего уровня АСУ ТП, являющиеся, по сути, связующим звеном между нижним и верхним уровнями АСУ ТП), уничтожена информация на АРМ (автоматизированных рабочих местах) диспетчерского персонала, DDoS-атакам (атакам, направленным на отказ в обслуживании) подверглись call-центры электросетевых компаний.

Результаты расследования кибератак, за которыми последовало отключение напряжения на семи подстанциях 110 кВ и 23 подстанциях 35 кВ и отключение энергоснабжения в пяти регионах страны на шесть часов, подвергались сомнению и вызвали множество догадок и предположений. Однако, оставив в стороне геополитические рассуждения и версии о злоумышленниках, обратим внимание на следующее: атаки Black Energy на энергосеть Украины были зарегистрированы еще в 2014 году. О возможных атаках на энергосеть предупреждали как минимум эксперты компании Eset. Год спустя инцидент произошел с участием того же Black Energy.

Если говорить о кибербезопасности в контексте защиты АСУ ТП, «предупрежден» еще совершенно не значит «вооружен». Могут пройти месяцы и даже годы, между тем, как офицер кибербезопасности – ответственный за ИБ АСУ ТП сотрудник – узнает о новых уязвимостях, возможных методах атаки и «защитных» патчах для программного обеспечения АСУ ТП и тем, как эти патчи действительно будут установлены. Установка обновлений на технические средства, работающие в режиме 24/7, связана с простоями и рисками сбоев после обновлений, недопустимыми на большинстве технологических объектов.

Впрочем, и в «корпоративной части» таких объектов не все гладко с обновлениями. Например, в апреле 2016 года в «офисной» сети немецкой атомной электростанции Gundremmingen было обнаружено многочисленное вредоносное программное обеспечение, включая W32.Ramnit и Conficker. Оба эти вредоносных червя известны с 2008 года и блокируются практически любым антивирусным программным обеспечением… Конечно, при его наличии и хотя бы ежегодном обновлении.

Инциденты, произошедшие в недалеком прошлом, хорошо демонстрируют уязвимость объектов ТЭК не только перед целенаправленны-

ми атаками, как в случаях с энергосистемой Украины или ядерной программой Ирана, но и перед нарушениями в работе, вызванными «случайным» заражением «обычным» вредоносным программным обеспечением.

О ТОМ, ЧТО ЕСТЬ

Еще пять лет назад обеспечение кибербезопасности промышленных объектов и объектов ТЭК было темой, интересной только узкому кругу специалистов. Сегодня ситуация меняется. За эти годы многие владельцы объектов провели аудиты безопасности, продемонстрировавшие уязвимости в инфраструктуре объектов, архитектуре систем и выстроенных или вообще отсутствующих процессах кибербезопасности.

Рисков и проблем кибербезопасности на объектах электроэнергетики очень много. В том числе и системного характера, которые характерны для большинства современных промышленных объектов и объектов топливно-энергетического комплекса. Основываясь на результатах многочисленных аудитов, могу выделить такие основные и наиболее распространенные проблемы:


12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

Рис. 1. Информационное сообщение «Киевоблэнерго» о хакерских атаках

- Недостаточность (или отсутствие) политик, процедур и процессов кибербезопасности.

  Зачастую политика информационной безопасности на объекте де-факто, а иногда и де-юре не распространяется на технологические системы. Это приводит к тому, что в технологических средах не соблюдаются даже элементарные принципы безопасности.

- Уязвимости сетевой архитектуры.

  На большинстве технологических объектов сетевая архитектура строилась, модернизировалась и развивалась в течение десятилетий. Причем процесс этот далеко не всегда учитывал требования информационной безопасности и

Рис. 2. Открытый шкаф системы городского освещения

чаще всего проходил по принципам «быстрее, доступнее, проще и надежнее». При этом идеологи и руководители процессов развития сетей связи менялись, привнося свое понимание этих принципов, а контроля со стороны регуляторов и нормативной базы как такового не было. Кроме того, многие изменения в сетевой архитектуре документированы очень скудно или не документированы вообще. Тщательный аудит часто приводит к неожиданным находкам – например, незащищенный удаленный доступ к SCADA-серверам из дома ответственных сотрудников или наличие неконтролируемых каналов связи между сетями среднего уровня АСУ ТП со смежными организациями (между двумя высоковольтными подстанциями, принадлежащими разным организациям).

■ Уязвимости процессов аутентификации, авторизации и регистрации событий.

Процессы управления и разграничения доступа в технологических сегментах зачастую управляются подразделениями, ответственными за эксплуатацию расположенных в этих сегментах систем. Поэтому привычными для специалистов по ИБ принципами и требованиями, такими как ограничение и разграничение полномочий, процедура смены паролей, ролевая модель доступа, регистрация и учет действий пользователей, зачастую пренебрегают. Причем это же пренебрежение правилами управления доступом иногда распространяется и на временно предоставляемый подрядчикам из внешних организаций доступ к технологическим системам.

■ Отсутствие средств защиты от вредоносного программного обеспечения.

Причин для нелюбви эксплуатирующих АСУ ТП подразделений к антивирусному ПО более чем достаточно. Среди них и опасение за возможные программные конфликты и сбои, которые может вызвать несовместимость с программным обеспечением АСУ ТП, и риск ложноположительных срабатываний, и опасение за нехватку вычислительных ресурсов аппаратного обеспечения. Действительно, многие системы объектов топливно-энергетического комплекса не могут похвастаться мощным и современным аппаратным обеспечением, а большинство антивирусного ПО, разработанного для корпоративных сред, достаточно требовательно к ресурсам. Также действительно существуют риски несовместимости ПО и ошибок первого рода (ложноположительных срабатываний антивирусного ПО на вполне легальные процессы и файлы). Однако следует учитывать, что существует антивирусное программное обеспечение, разработанное специально для применения в технологических средах и протестированное разработчиками систем АСУ ТП, а аккуратное и тщательное конфигурирование квалифицированными экспертами позволяет свести риски к минимуму. В то же время распространение по технологической сети «древних» вирусов может привести к куда более неприятным последствиям.

■ Уязвимости или недостаточность контроля и защиты физического и логического периметра.

Если говорить об объектах ТЭК и, в частности, электроэнергетики, то «размазанность» логического периметра – это часто встречаемое явление. Каналы связи с системным оператором (ОДУ, РДУ), со смежными объектами других организаций, с подрядчиками и другими внешними системами зачастую никак не защищены. Для распределительных сетей характерно расположение объектов в «слабоконтролируемой» зоне – например, системы телемеханики в помещениях РТП (распорядительные трансформаторные подстанции) или коммуникационное оборудование, устанавливаемое

в жилых домах. Элементы системы управления внешним городским освещением часто располагаются в общедоступных местах – в шкафах, которые даже не всегда запираются (см. рис. 2). В шкафу на приведенной фотографии нет средств автоматизации, но короткое замыкание может устроить любой желающий. Практически каждая крупная распределенная технологическая система имеет характерные уязвимости, связанные с недостаточным обеспечением безопасности периметра.

Самая основная проблема кибербезопасности – отсутствие ответственных за нее.

Как правило, на объектах встречаются два варианта проблемы:

1 Ответственного за ИБ (или кибербезопасность) в технологических сегментах просто нет. «Связисты» отвечают за то, чтобы «связь была», «асутэпэшники» – за то, чтобы «АСУ ТП работала», а вот кто отвечает за то, чтобы «АСУ ТП не работала на злоумышленника», совершенно неясно.

2 Ответственный за ИБ «как бы» есть, но он не обладает ни компетенцией и квалификацией, ни возможностями влияния на архитектуру, конфигурацию или порядок работы систем связи и АСУ ТП. В этом случае на объекте могут присутствовать организационные меры кибербезопасности, соблюдаемые в технологических сегментах весьма формально. При этом требования информационной безопасности могут не учитываться ни при модернизации или создании новых систем, ни при их эксплуатации.

Оба эти варианта ведут к тому, что на объекте невозможно выстроить процедуры и процессы безопасности, разработать, внедрить и контролировать организационные меры защиты, и даже самые совершенные технические средства защиты, внедренные самыми квалифицированными подрядчиками, будут бесполезны – станет некому управлять ими и некому расследовать и реагировать на инциденты. Пока эта проблема не будет решена, пока не будет создано ответственное за обеспечение кибербезопасности подразделение, обладающее соответствующей компетенцией и правами, эффективность остальных мер защиты всегда будет под большим вопросом.

О ТОМ, ЧТО, ВОЗМОЖНО, БУДЕТ

В октябре 2016 года в рамках IV Международной конференции по защите АСУ ТП «Время действовать вместе» состоялся турнир по Industrial CTF – соревнования по кибербезопасности, организованные «Лабораторией Касперского». В прошлом году участникам предстояло попробовать свои силы во взломе цифровой подстанции, которая, кстати, была успешно взломана. В этом году «на растерзание» дан «целый город»: смоделированы и генерация электроэнергии, и распределение, и потребители. Электроснабжение «города» тоже было нарушено разными методами.

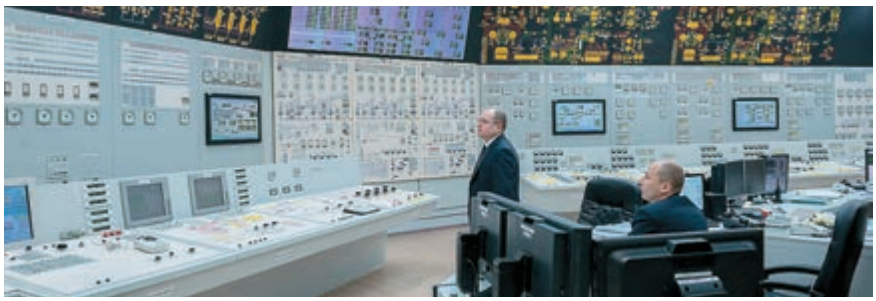
Средний возраст участников соревнований – «хакеров» – в среднем не больше 25 лет. Опыта работы в электроэнергетике и глубоких познаний в АСУ ТП и РЗА у большинства команд, успешно взломавших стенды, также нет. Это демонстрирует тот факт, что опыта тестирований на проникновения в корпоративных системах, знания «классических» информационных и сетевых технологий и информации из открытых источников достаточно для совершения успешных атак на объекты АСУ ТП. Древний миф о том, что «для взлома АСУ ТП нужны особые знания, навыки и помощь спецслужб», теперь развенчан.

Популярность кибербезопасности АСУ ТП и атак на промышленные системы растет и будет расти с каждым годом. Это означает, что помимо роста компетенции экспертов, развития систем защиты и усложнения атак нас ожидает рост числа так называемых script-kiddies в сфере атак на АСУ ТП – молодых, не очень умелых, но достаточно активных злоумышленников, пытающихся взламывать все, что попадется под руку, по готовым алгоритмам и схемам ради развлечения и не задумываясь о последствиях. В большинстве случаев они будут использовать известные уязвимости и детектируемое вредоносное программное обеспечение. Но такие атаки все равно могут стать проблемой для объектов электроэнергетики.

С другой стороны, автоматизация объектов ТЭК и открываемые ею новые горизонты для кибервойны являются чересчур лакомым кусочком для террористических организаций и спецслужб недружественных стран, чтобы их игнорировать. И так как степень автоматизации объектов ТЭК в дальнейшем будет только расти, риски, связанные с кибератаками на эти объекты, также будут повышаться.

ИДТИ ДО КОНЦА

За последние несколько лет ситуация в сфере кибербезопасности технологических объектов и объектов ТЭК немного поменялась. Владельцы многих объектов перешли от стадии отрицания («наша АСУ ТП полностью изолирована от внешнего мира», «для взлома АСУ ТП требуются особые, очень глубокие и специализированные знания и навыки» и даже «наш объект никому не интересен, нас некому атаковать») к стадии торга. На многих объектах уже проведен аудит безопасности и выявлены проблемы, но владельцы и заинтересованные стороны еще решают, как эти проблемы можно устранить с минимальными потерями для бюджета и рисков прерывания технологических процессов. Сложно оценить некий «общий уровень защищенности объектов ТЭК России» и его изменения за несколько лет, но очевидно, что процессы кибербезопасности запущены и их не остановить, так же как и не остановить процессы развития угроз. ТЭК



> «Зачастую политика информационной безопасности на объекте де-факто, а иногда и де-юре не распространяется на технологические системы