Некоммерческое партнёрство
«НАУЧНО-ТЕХНИЧЕСКИЙ СОВЕТ
Единой энергетической системы»

109044 г. Москва, Воронцовский пер., дом 2
Тел. (495) 912-1078, 912-5799, факс (495) 632-7285
E-mail: dtv@nts-ees.ru, http://www.nts-ees.ru/

УТВЕРЖДАЮ
Председатель Научно-технической коллегии НП «НТС ЕЭС», д.т.н., профессор
_____ Н.Д. Рогалёв
«23» ноября 2017 г.

ПРОТОКОЛ

заседания секции «Информационные технологии» НП «НТС ЕЭС» по теме:
«Имитационное моделирование, как инструмент оценки защищённости ИТ инфраструктуры и оптимизации затрат на обеспечение ИБ».

09 ноября 2017 года № г. Москва

Присутствовали:

Всего: 10 чел.

Со вступительным словом выступил председатель секции «Информационные технологии», заместитель директора по информационным технологиям Филиала АО «СО ЕЭС» Московское РДУ И.А. Щипицин.

С докладом «Имитационное моделирование, как инструмент оценки защищённости ИТ инфраструктуры и оптимизации затрат на обеспечение ИБ» выступил начальник Аналитического отдела АО «РТСофт» Литвинов П.В.

В своём докладе Литвинов П.В. отметил следующее:

1. В вопросах планирования обеспечения безопасности энергообъекта можно опираться на логику, аналогичную заложенной в пирамиде Маслоу для психологии: в первую очередь должны быть выполнены все требования регуляторов, затем обеспечена катастрофоустойчивость объекта, затем уже идут структурная надежность, ситуационная осведомленность и эффективность затрат. Из чего следует, что необходимо научно-обоснованное планирование затрат на ИБ. Требуется «балансировка» расходов между рисками ИБ и другими техническими рисками, человеческим фактором и т.п. поскольку безопасность может быть достигнута только пропорциональным выполнением всего комплекса мероприятий, а бюджет всегда ограниченный.

2. Особенностью планирования в энергетике является необходимость составления долгосрочных планов, поскольку сроки службы первичного оборудования и большинства активов составляют десятки лет. С целью соответствия этому требованию предлагается использовать результаты выполнения расчета на имитационной модели прогноза количества взломов на ближайшие 10 лет, построенной с применением метода системной динамики.

3. Участникам заседания была представлена концепция создания имитационной модели, выполняющей оценку изменения рисков во времени через динамику изменения количества киберугроз, числа устройств, мероприятий по защите, вероятности наличия уязвимостей и предполагаемого профиля злоумышленника и результаты расчета в разбивке по месяцам.

4. Имитационная модель является развитием темы внутреннего НИР АО «РТСофт», первые результаты которого были представлены на

конференции «Релейная защита и автоматика энергосистем 2017» в апреле 2017 в Санкт-Петербурге и впоследствии на Международном коллоквиуме исследовательского комитета D2 СИГРЭ в сентябре этого года в Москве.

5. Также были изложены предложения по способу расчета метрик текущего состояния защищенности, основанные на определении размерности объекта и его потенциальных уязвимостей, образующих «поверхность для атаки». Принципиально важным является организация запуска процедуры пересчета при каждом изменении таких параметров, как:

– количество, виды и состояние оборудования;

– численный состав персонала, его квалификация, роли и обязанности;

– конфигурация сети и ее сегментирование;

– новые сведения в базах данных уязвимостей.

Следуя описанной методологии, можно получить нужное количество, как независимых метрик, так и производных от них KPI, ориентированных на принятие управленческих решений.

6. В заключение были предложены способы развития модели, с целью учета большего числа влияющих факторов посредством:

a. перехода к агентному моделированию. В настоящее время в модели рассматривается усредненный портрет "хакера" или "устройства", как функция времени. Создавая достаточное число агентов и устанавливая характеристики и правила взаимодействия для каждого из них в каждый момент времени, мы можем получить новые, совсем не очевидные зависимости.

b. параллельного использования и учета отдельных значимых факторов через дискретно-событийное моделирование. Например, таких, как ввод в работу Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

В обсуждении доклада приняли участие: заместитель директора по информационным технологиям Филиала АО «СО ЕЭС» Московское РДУ Щипицин И.А., д.т.н., начальник департамента методов и средств управления АО "Институт "Энергосетьпроект" Наровлянский В.Г., д.т.н., заведующий отделом ОАО «НТЦ ФСК ЕЭС» Рабинович М.А., руководитель проектов ООО «Ай-Ти Энерджи Сервис» Гришин О.С.

Обсуждались вопросы:

– в какой степени предложенная модель учитывает специфику электроэнергетических компаний;

– использование доработанной модели для расчета надежности и устойчивости к киберугрозам оборудования конкретного объекта;

– наличие зарубежных аналогов и планов по развитию модели;

– границы применимости и оценка точности расчетов.

Отметили:

Возможность использования представленной методологии и инструментария для решения аналогичных или смежных задач.

Целесообразность разработки технологии передачи модели и (или) результатов расчета потенциальным заказчикам с учетом требований предъявляемым 187-ФЗ.

Заслушав доклад и выступления участников дискуссии заседания, заседание решило:

1. Принять доклад к сведению.
2. Отметить научную новизну и прикладной характер выполненного НИР, особенно актуального в связи с вступлением в силу с 1 января 2018 г. Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

3. Рекомендовать предложенную методологию субъектам электроэнергетики, как один из инструментов долгосрочного планирования мероприятий по обеспечению информационной безопасности и оценки безопасности критической информационной инфраструктуры.

Первый заместитель Председателя Научно-технической коллегии НП «НТС ЕЭС», д.т.н., профессор

В.В. Молодюк

Председатель секции «Информационные технологии» НП «НТС ЕЭС», заместитель директора по информационным технологиям Филиала АО «СО ЕЭС» Московское РДУ

И. А. Щипицин

Ученый секретарь Научно-технической коллегии НП «НТС ЕЭС», к.т.н.

Э.Ш. Исамухамедов

Секретарь секции «Информационные технологии» НП «НТС ЕЭС»

Е.О. Базилюк