

[Поиск](#)

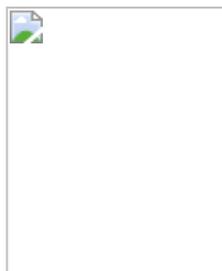
- [О ПИР-Центре](#)
- [Публикации](#)
- [Научные проекты](#)
- [Образование](#)

[Вход](#)[Версия для печати](#)[Карта сайта](#) | [Обратная связь](#) | [Архив сайта](#)[English](#)

Письмо: PIR PRESS NEWS - Internet as a critical infrastructure: what to defend, how and from whom?

20.11.2016

PIR PRESS NEWS - Internet as a critical infrastructure: what to defend, how and from whom?



МОСКВА, 21 НОЯБРЯ 2016. ПИР-ПРЕСС – «Мы сталкиваемся с угрозой повторения ситуаций, когда специально разработанные средства программного обеспечения оказываются способны преодолеть даже физическую изоляцию сетей. В этих условиях нам интересно и важно понимать, что делается и как развивается реакция регуляторов, отрасли, рынка и, в конечном итоге, международная реакция на новые вызовы и угрозы», – Олег Демидов, консультант ПИР-Центра.

Проблема кибербезопасности объектов критической инфраструктуры была одной из самых обсуждаемых на [Международной конференции «Повестка 21 века – новые технологии и вызовы глобальной безопасности»](#), состоявшейся в Москве 28 сентября 2016 года. Среди выступающих были как эксперты, так и представители профессионального технического сообщества, поставщики решений информационной безопасности, что позволило составить многомерную картину существующей ситуации. Модерировал сессию консультант ПИР-Центра **Олег Демидов**.

Пленарное заседание открыла директор InfoWatch Наталья **Касперская**, обозначив сложности, с которыми сталкиваются вендоры на разных этапах своей работы. Трудности касаются как взаимодействия с клиентами и регуляторами, так и недостаточной зрелости «промышленного Интернета вещей» как концепции. «Поскольку промышленный Интернет вещей на сегодняшний день новая технология, которая внедряется практически без систем защиты, я бы сказала, что предприятия, которые стремятся внедрить её у себя, находятся сейчас в более уязвимом положении, чем те, которые подходят к этому вопросу консервативно», – подчеркнула Наталья Касперская.

Андрей Суворов, директор по развитию бизнеса безопасности критической инфраструктуры «Лаборатории Касперского», рассказал об основных отличиях защиты корпоративных сетей и сложных киберфизических систем инфраструктурных объектов. В последнем случае «очень важно обеспечить устойчивость технологического процесса», отметил Суворов. Эксперт далее остановился на сложности в распознавании угроз подобным системам: «Недостаточно знать, есть ли вирус на компьютере – важно понимать аномальное поведение в рамках технологического процесса».



Выступающие не обошли стороной и тему развития рынка решений безопасности для промышленных объектов, а также проблему несоответствия между спросом и предложением в этой сфере. «Большинство продуктов вендоров решает точечную задачу. А бизнес, как правило, заинтересован в комплексном решении, и именно объединяя решения, можно создать новые продукты», – сформулировал ключевое противоречие руководитель направления «Технологии информационной безопасности» фонда «Сколково», Сергей **Ходаков**, рассказывая о поддержке фондом начинающих ИТ-компаний.



Заседание завершилось выступлением консультанта по кибербезопасности Вадима **Подольного**. Эксперт отметил, что защита от киберугроз автоматизированных систем управления технологическими процессами (АСУ ТП) уже занимает важное место при проектировании и строительстве АЭС: «АСУ ТП – это 10% от стоимости АЭС, а 10% от стоимости АСУ ТП – деньги, которые вкладываются в кибербезопасность». По мнению спикера, немалое значение имеет разработка стандартов в области кибербезопасности атомных электростанций и деятельность МАГАТЭ в этой области. По его словам, документ, описывающий зонную модель безопасности АЭС, сейчас находится в стадии разработки и увидит свет в 2017 году.



На заседании также был представлен совместный доклад ПИР-Центра и Centre russe d'études politiques «Кибербезопасность гражданских ядерных объектов: оценка угроз и определение дальнейших шагов». Резюме доклада, а также другие материалы по данной теме можно найти на странице проекта ПИР-Центра [«Кибербезопасность объектов критической ядерной инфраструктуры»](#).

Презентации и тексты выступлений участников конференции доступны на сайте <http://conference2016.pircenter.org>

Тел.: +7 (495) 987-19-15

Адрес для писем: Россия, 119019, Москва, а/я 147

ПИР-Центр 2022 год. Все права защищены.

Разработан ИССАрт.

loading

[Ошибка?](#)

Обратите внимание на оши