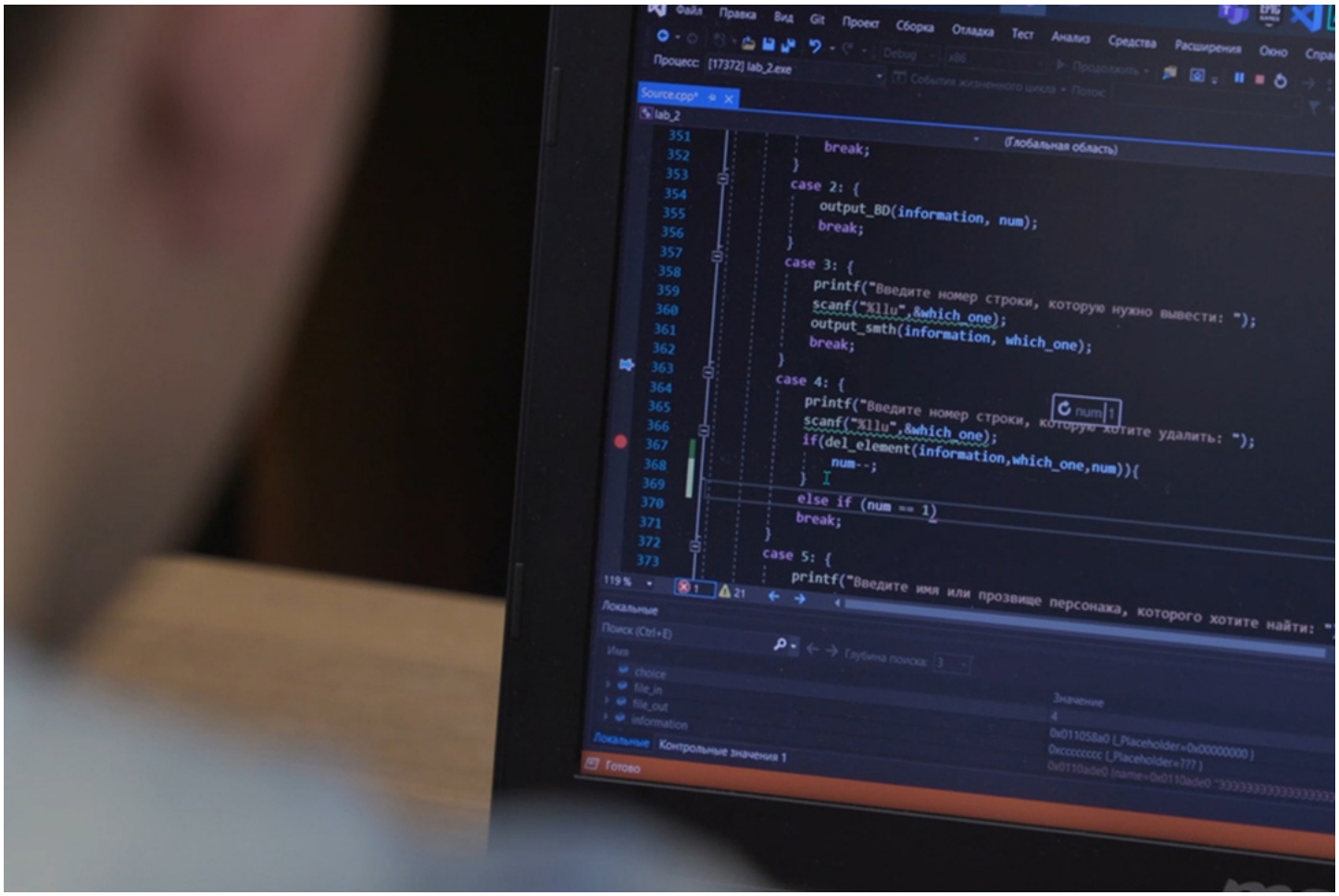
Ученые защитят «Умный город» от киберугроз



Санкт-Петербург, как и другие города России, активно участвует в формировании программы «Умный город», которая будет предоставлять новые услуги для жителей мегаполисов, повышая безопасность граждан. Неотъемлемой частью такой системы являются цифровые сервисы. Благодаря системам Интернета вещей (IoT) окружающая среда способна самостоятельно адаптироваться под желания человека. Для такой инфраструктуры особенно актуальны угрозы кибербезопасности.

Специалисты Санкт-Петербургского политехнического университета Петра Великого разработали методику оценки киберрисков в интеллектуальных системах умного города. Апробация разработанной методики проведена на испытательном стенде «умный перекресток» (компоненте интеллектуальной транспортной системы умного города). Результаты работы опубликованы в научном журнале "Machines" издательства MDPI.

Ученые отмечают, что у киберпреступников появились новые цели — нарушение процессов функционирования крупных предприятий и городской инфраструктуры, а также перехват управления ими. Злоумышленники, использующие беспроводные каналы, могут удаленно вторгаться в целевую подсеть или в устройство (группу устройств), перехватывать трафик, запускать атаки типа «отказ в обслуживании» (в том числе распределенные) и захватывать управление над устройствами Интернета вещей для создания бот-сетей.

«В настоящее время традиционные стратегии анализа киберрисков не могут быть напрямую применены при построении и оценке цифровых инфраструктур умного города, так как новая сетевая инфраструктура является неоднородной и динамической. Цель нашего проекта — обеспечить уровень защищенности информационных активов умного города с учетом специфики современных киберугроз», — отмечает научный сотрудник Института кибербезопасности и защиты информации СПбПУ Василий Крундышев.

В СПбПУ создана методика анализа рисков кибербезопасности умного города, включающая этапы идентификации типов активов, идентификации угроз, расчет рисков и анализ полученных значений рисков. Предлагаемая методика базируется на количественном подходе, при этом является легко и быстро вычислимой, что особенно важно в условиях функционирования современных динамических инфраструктур. Экспериментальные исследования с использованием комплекса разработанных имитационных моделей типовых цифровых инфраструктур умного города (Интернет вещей, умное здание, умный перекресток) продемонстрировали превосходство предложенного авторами подхода над существующими отечественными и зарубежными аналогами.

В ближайшем будущем планируется автоматизировать расчет рисков кибербезопасности в умном городе на основе разработанной методики.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90001.