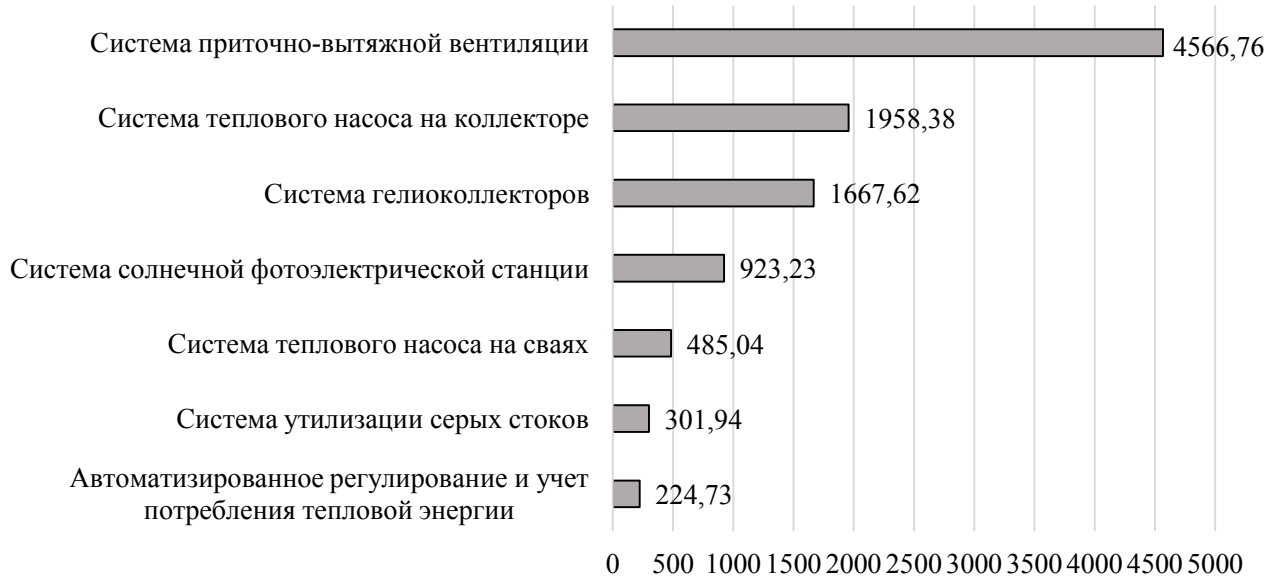

Рисунок 1 – Среднее арифметическое значение инвестиционных затрат на реализацию мероприятий повышения энергоэффективности жилых домов в расчете на 1 квартиру, долларов США [4]

Работы по повышению энергоэффективности, автоматизация и диспетчеризация в экспериментальных жилых домах увеличили стоимость их возведения на 21,3% – 32,7% стоимости строительства аналогичных жилых домов. По классу интеллектуальности такие дома можно отнести ко 2-му классу (эконом).

Основными факторами, влияющими на экономическую эффективность, являются инвестиционные затраты; производительность систем; эксплуатационные расходы на обслуживание систем и их энергопотребление; тарифы на энергоресурсы; поведение жильцов, обеспечивающее использование или не использование систем.

Реализация проекта строительства трех энергоэффективных жилых домов позволила осуществить ряд уникальных для Республики Беларусь мероприятий, обеспечивающих повышение энергоэффективности.

С экономической точки зрения интеллектуализация зданий, повышение их энергоэффективности, обеспечивающие развитие жилого фонда Республики Беларусь в рамках концепции «Умный дом», «Умный город» требует увеличения капитальных затрат, связанных с внедрением систем. Чем выше степень интеллектуализации зданий и сооружений, тем выше уровень единовременных затрат. Экономическая эффективность на уровне отдельно взятого дома определяется экономией в первую очередь тепловой и электрической энергии, а также экономией расхода воды, потребляемых в процессе эксплуатации, на уровне «Умных городов» – экономией удельных затрат на обслуживание коммунальных сетей и жилищного фонда города в целом. Однако эти затраты обеспечивают достижение целей создания умных городов: новое качество жизни населения, что обеспечивает социальную стабильность общества, раскрытие потенциала населения, безопасной и комфортной среды обитания человека.

УДК 004.056.5

АНАЛИЗ СЕТЕВЫХ УЯЗВИМОСТЕЙ РАЗЛИЧНЫХ УСТРОЙСТВ С ДОСТУПОМ В ИНТЕРНЕТ В АДРЕСНЫХ ПРОСТРАНСТВАХ МИНСКА И САНКТ-ПЕТЕРБУРГА

Грандилевский А.И.
Санкт-Петербургский горный университет

Аннотация. *Использованы методы массового сканирования диапазонов IPv4 адресов, для определения уровня безопасности сетевых машин в Санкт-Петербурге и Минске. Установлен высокий уро-*

вень риска потенциальных повреждений (в.т.ч. взломов, неправомерного получения доступа, кражи персональных данных и т.д.).
Ключевые слова: *уязвимость, интернет, сканирование, TCP/IP, IPv4, веб безопасность.*

Введение. Невозможно представить современный мир без обилия технических устройств и компьютерных технологий в целом. И с каждым днем технологии шагают вперед все быстрее и быстрее. Немалую роль в возможности подобных скоростей прогресса сыграло появление Всемирной Глобальной Сети или Интернета. Прошло уже почти 50 лет с момента, когда была запущена первая сеть, что считается днем рождения интернета.

Когда мы говорим о взаимодействии различных устройств, мы понимаем, что они должны быть каким-либо образом соединены между собой для обмена некой информацией. В случае прямого локального подключения для двух или более устройств нет нужды использовать особые правила, если мы хотим передать информацию всем подключенным устройствам. Достаточно передать ее на вход и на выходе она будет получена другим устройством. Но как быть с Глобальной Сетью, в которой, по подсчётам аналитического агентства We Are Social [1], к 2019 году насчитывается уже более 4 млн. устройств с различными структурами, ОС и способами работы с сетью? Для организации взаимодействия между всеми этими агрегатами был разработан ряд правил, называемых сетевой моделью. В рамках сетевой модели правила взаимодействия именуются протоколами, поэтому сетевую модель иногда могут называть стеком (набором) протоколов. Наибольшую актуальность на сегодняшний день имеет сетевая модель TCP/IP (от англ. Transmission Control Protocol / Internet Protocol). Модель является открытой и общедоступной, а ее систематизацией и развитием занимается международное открытое сообщество Инженерный совет Интернета (англ. IETF / Internet Engineering Task Forge).

Исследование. Стек протоколов TCP/IP является, по сути, концептуальной моделью и набором правил маршрутизации, состоящий из 4 уровней: Прикладной (Application Layer), Транспортный (Transport Layer), Межсетевой(Network Layer) и Канальный(Internet Access Layer). В рамках моего исследования я затрону Прикладной и Транспортный уровни, наборы протоколов на которых я буду использовать и исследовать.

В основе передачи данных по сети Internet лежит система IP-address, позволяющая присвоить уникальный идентификационный номер любому устройству в сети. Занимаются этим Региональные Интернет Регистраторы (англ. RIR/Regional Internet Registrator), подразделение Администрации адресного пространства Интернет (англ. IANA/Internet Assigned Numbers Authority), межнациональные некоммерческие организации, которые выделяют государствам и территориям определённые зоны в адресном пространстве IP. Мое исследование касается только IP-адресов на территории городов Санкт-Петербурга и Минска в рамках протокола IPv4, полный список которых предоставляется в свободном доступе в соответствии с принципами сообщества IETF.

Технология TCP, как и UDP, используют т.н. порты, «дырки» доступа в сеть для ПО. В соответствии с портом стек протоколов может идентифицировать процесс получатель и применить соответствующий протокол Прикладного уровня в пределах одного хоста, т.е. конечного устройства. Каждая программа или процесс использует свой порт, выделяемый ей системой или заданный программно. Существует ряд портов, использующихся системой для определенных специфических целей. Такие порты называются общеизвестными, выделяются и регистрируются IANA. В исследовании будут протестированы на возможность доступа и взаимодействия ряд общеизвестных портов, отвечающих за конкретные протоколы взаимодействия.

Сканирование для исследования было проведено с использованием терминальных команд OS Manjaro 19.2.115 на базе ядра Arch Linux и утилиты masscan, а также поисковика Shodan.io. Для проведения исследования была использована адаптированная к целям исследования методика, предложенная Christian Haschek [2]. Результаты сканирования представлены в таблице 1.

Таблица 1 – Результаты сканирования

		Минск		Санкт-Петербург	
Общее количество IP4 доменов		68098		348613	
Порт 445	Открытый порт	число	% относительно всех устройств	число	% относительно всех устройств
		148	0,2%	2205	0,6%
	Уязвимость Ethernalblue	81	0,1%	1078	0,3%
Порт 53	Открытый порт	2356	3%	15224	4%
	Являются open resolver	402	0,6%	3212	1%
Порт 80	Общее число	9101	13%	38014	11%
	Устаревшие	27	0,04%	1071	0,003%
Иные устройства, не защищенные системой		4 веб камеры, 2 принтера, 2 домофона, 3 диктофона		34 веб камеры, 8 принтеров, 2 системы умный дом, 4 домофона, 1 диктофон	

Порт 445 зарегистрирован за протоколом MICROSOFT-DS в Windows 2000 и более поздних версиях и используется для прямого доступа к сети без использования NetBIOS и алгоритмов безопасности.

Использованные команды:

masscan –p445 –tps300 –iL <city>.ips –oG 445.port.<city>.scan

Подобная прямая уязвимость в устройстве позволяет различным вредоносным эксплойтам получать полный доступ к системе и запускать произвольный код. К примеру, в 2017 году была открыта уязвимость CVE-2017-0144, названая кодовым именем Ethernalblue, воздействующая на этот порт. Компания Microsoft выпустила «патч вчерашнего дня», исправляющий уязвимость на все версии Windows, даже поддержка которых была уже прекращена.

Использованные команды:

nmap -p 445 -Pn --script smb-vuln-ms17-010 <targethosts> -oG Ethernalblue.<city>.scan

Сервера с открытым портом 53 в системе UDP является уязвимым к атакам типа DoS (Denial of Service), если устройства являются open-resolver, т.е. принимают рекурсивные DNS-запросы с любой точки сети. Такая атака называется HTTP-флуд, и её принцип заключается в отправке небольшого пакета данных, на который уязвимый сервер отвечает пакетом в десятки раз большего объёма, загружая свой канал. В определенный момент пропускная способность сервера оказывается меньше потока данных, что вызывает критические ошибки. DoS-атаки используются для отключения сервера, перехватывания контроля над системой или получения информации о системе, доступ к которой может открываться в случае критических ошибок.

Поиск подобных серверов возможно осуществить в два шага.

Использованные команды: *masscan –pU 53 –iL <city>.ips –oG 53.port.<city>.scan*

Первым шагом осуществляется сканирование машин с открытым портом 53. Полученный результат можно проверить и отфильтровать на open-resolver признак с помощью терминальной команды dig и сайта открытого источника openresolver.com, позволяющего провести соответственное сканирование.

Порт 80 является стандартным для протокола http и используется для загрузки веб-страниц и серверных частей.

Использованные команды: *masscan –p80 –iL <city>.ips –oG 80.port.<city>.scan*

С помощью инструмента nmap получена статистика по видам веб-серверов. В Минске, как и в Санкт-Петербурге nginx является наиболее популярным (1698 из 9101 и 8316 из 38014 соответственно), что свидетельствует о достаточно высоком уровне квалификации и информированности специалистов, поскольку nginx на сегодняшний день представляет собой наиболее актуальный и современный инструмент управления серверами. В то же время в обоих городах существует ряд машин с устаревшим и необслуживаемым ПО, к примеру, WinCE, поддержка и обслуживание которой уже прекращено.

С помощью инструмента сканирования Shidan.io были обнаружены множество камер видеонаблюдения, принтеров и других устройств с подключением к сети со свободным доступом, без какой-либо защиты.

Таким образом, как видно из таблицы 1, установлен высокий уровень риска потенциальных повреждений (в.т.ч. взломов, неправомерного получения доступа, кражи персональных данных). Результаты сканирования достоверно не различаются как по адресному пространству Минска, так и Санкт-Петербурга в процентном соотношении ($p<0,05$). Критическим нарушением безопасности личного пространства и конфиденциальных данных являются возможность стороннего проникновения через различные видео и аудио устройства без защиты. В частности, в Санкт-Петербурге в момент сканирования были доступны 34 веб камеры, а в Минске 4.

Выводы. Способом устранения большинства найденных уязвимостей является простое совместное использование брандмауэра и фаервола. Полученная статистика позволяет сделать вывод, что держатели хостов достаточно плохо следят за безопасностью. Конечные пользователи, приобретая устройства с доступом к сети, (веб-камеры, принтеры или иное) не настраивают их надлежащим образом, оставляя полный доступ для любого участника Всемирной Сети. Конечный пользователь без соответствующей квалификации имеет возможность избежать всех описанных выше рисков при внимательном прочтении руководств по эксплуатации и инструкций к сетевому оборудованию.

Рекомендации. Наиболее уязвимыми единицами остаются устройства, использующие устаревшие и, зачастую, более не поддерживаемые программные продукты. Такие как WinCE, поддержка которой была завершена в 2013 году. Новые ошибки и возможности вредоносного использования открывают ежедневно, и, чтобы обеспечить безопасность интернет пространства необходимо своевременно узнавать о них и закрывать. Любому держателю сервера целесообразно организовать контроль и обеспечение безопасной работоспособности устройств с привлечением квалифицированного ИТ-специалиста или системного администратора в области веб безопасности. Это позволит снизить уровень риска для конечного пользователя.

УДК 334.02

МАЛЫЕ ИННОВАЦИОННЫЕ ПРЕДПРИЯТИЯ НА БАЗЕ ВУЗОВ КАК ИНФОРМАЦИОННЫЙ ИНСТРУМЕНТ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Грахов В.П., Кислякова Ю.Г., Симченко О.Л., Симакова У.Ф., Чазов Е.Л.
Ижевский государственный технический университет имени М.Т. Калашникова

На современном этапе развития общества для политической и экономической стабильности государства необходимым условием является способность создавать новые высокие цифровые технологии, внедрять их на рынок, то есть проектировать инновации в определенный вид продукта или услуги [1].

В течение последних лет в Российской Федерации (РФ) было принято несколько федеральных законов и постановлений правительства, которые призваны регламентировать совместную деятельность высших учебных заведений и малых инновационных предприятий [2].

На сегодняшний день Ижевский государственный технический университет имени М.Т. Калашникова (ИжГТУ) является крупным региональным научно-образовательным центром, базой для проведения фундаментальных и прикладных исследований для предприятий машиностроения, приборостроения, строительной отрасли, а также оборонно-промышленного комплекса РФ.

Создание инновационной инфраструктуры вуза представляет собой интегрирующую подсистему и является одним из базовых направлений развития и стимулирования национальной инновационной системы, долгосрочного роста экономики страны и достижения лидирующих позиций (рис. 1).