Кибербезопасность как новая сфера национальной безопасности Республики Беларусь

Васильев И. Г., студ. IV к. БГУ,
науч. рук. проф. Свилас С. Ф., д-р ист. наук, доцент

Кибербезопасность – стратегическая проблема государства, комплексно затрагивающая экономику страны. Как и любая другая сфера государственных интересов, кибербезопасность требует слаженных действий всех элементов системы национальной безопасности. Для качественной защиты ресурсов в сфере кибербезопасности требуется постоянный контроль, обработка и анализ новых рисков, прогнозирование направления кибератак и совершенствование систем безопасности.

Всевозможные структуры и предприятия используют информационные технологии для сбора, обработки и хранения информации, включающей в себя персональные данные клиентов и сотрудников. Данная информация является конфиденциальной, подвержена различным угрозам, и ее утечка может иметь негативные последствия как для отдельной персоны, так и для экономики всего государства. Наибольшей опасности подвержены организации и предприятия, которые непосредственно поддерживают инфраструктуры целых государств, областей и городов. Их называют критическими инфраструктурами [3]. К ним причисляют: снабжение водой, электричеством, теплом; здравоохранение; транспорт; переработка отходов.

Сложность работы критических инфраструктур объясняется целостностью их устройства, взаимозависимостями между собой и разными уровнями системы. В этом же и заключается основная опасность – критические инфраструктуры склонны к каскадным инцидентам; при нарушении работы одного из уровней работы критической инфраструктуры вся система перестает работать должным образом.

Критические инфраструктуры могут служить источниками катастроф, аварий, терактов, поэтому считается, что они – основная область, подлежащая дальнейшим модернизациям кибербезопасности. Главная проблема в обеспечении кибербезопасности – время. Технологии, методики и принципы проведения кибератак совершенствуются каждый день. Понимая это, можно считать, что традиционных подход, заключавшийся в защите лишь самых важных ресурсов от внешних, уже известных угроз, более не является актуальным.

Согласно Целям в области устойчивого развития, обновленными ООН в 2018 г., Республика Беларусь находится на 69 месте в рейтинге глобальной кибербезопасности [1], государству не хватает оперативных центров реагирования на инциденты в сфере кибербезопасности [2; 5]. Существующие регуляторы, включая недавно образованный Национальный центр реагирования

на компьютерные инциденты, обеспечивают лишь защиту «по факту», уже после нанесения удара. В стране не существует компетентного органа, который занимался бы оценкой, анализом и прогнозом вероятных угроз, а также органа, вырабатывающего рекомендации по обеспечению безопасности интернет-ресурсов.

Позиции принятой в 2019 г. Концепции информационной безопасности [4] уже в 2020 г. перестали соответствовать необходимому минимуму кибербезопасности и защиты информационного пространства государства, идет разработка принципов деятельности будущего органа, противодействующего киберугрозам в реальном времени и в перспективе. Инвестиции в сферу кибербезопасности растут в геометрической прогрессии из года в год, навыки по защите данных считаются одними из самых перспективных во всем мире.

Кибербезопасность базируется на весьма специфическом классе моделей процессов обработки информации, и в этой сфере уже третий год наблюдается кадровый голод. Беларусь большей частью зависит от иностранных производителей программного обеспечения и инфокоммуникационных решений, отсутствие отечественных разработок в этой сфере вынуждает использовать импортные аналоги.

Дальнейшее обеспечение кибербезопасности республики напрямую зависит от уровня взаимодействия заинтересованных участников: государство, научно-исследовательские институты, разработчики, производители и провайдеры инфокоммуникационных решений, регуляторы, заказчики и потребители. В качестве возможного решения и в целях организации структур, специализирующихся на анализе решенных и прогнозе будущих угроз в сфере кибербезопасности, предлагается организовать ряд системных НИОКР, а также объединить существующие регуляторы в одну структуру с общей целью и ответственностью. Данная модель позволит государству на требуемом уровне формировать защищенное информационное пространство, а также обеспечить развитие экономики путем увеличения количества рабочих мест и объема производства отечественных инфокоммуникационных решений.

Литература

1. Global Cybersecurity Index 2018 [Электронный ресурс]. – Режим доступа: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. – Дата доступа: 08.04.2021.

2. В сети опубликованы данные белорусских милиционеров [Электронный ресурс]. – Режим доступа: https://www.securityvision.ru/blog/kii-chto-eto. – Дата доступа: 09.04.2021.

3. КИИ – что это? [Электронный ресурс]. – Режим доступа: https://belnovosti-by.turbopages.org/belnovosti.by/s/obshchestvo/hakery-prodolzhayut-vzlamyvat-gosudarstvennye-sayty-v-belarusi-spisok-atakovannyh. – Дата доступа: 09.04.2021.

4. Концепция информационной безопасности Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf. – Дата доступа: 09.04.2021.

5. Хакеры продолжают взламывать государственные сайты в Беларуси: список атакованных ресурсов [Электронный ресурс]. – Режим доступа: https://belnovosti-by.turbopages.org/belnovosti.by/s/obshchestvo/hakery-prodolzhayut-vzlamyvat-gosudarstvennye-sayty-v-belarusi-spisok-atakovannyh. – Дата доступа: 09.04.2021.

Mexico and the WTO Appellate Body Crisis

Глеков В. О., студ. IV к. БГУ,
науч. рук. доц. Пильгун Е. В., канд. филол. наук

The World Trade Organization (WTO) is an international multi-lateral organization, which was established back in the 1995 as a substitute to the older platform known as the General Agreement on Tariffs and Trade (GATT). The WTO's declares international trade liberalization and establishment of proper and clear rules of international trade as its primary aims. In order to reach these objections the WTO is made up of several bodies, including the WTO Secreteriat, the WTO General Council, Dispute Settlement Body and the Appellate Body. This paper concerns the crisis, which has emerged with the paralysis of the Appellate Body and the reaction to this crisis of one of the countries depending on the successful performance of the WTO – Mexico.

The WTO's Appellate Body Crisis

The WTO's Appellate Body is a permanent WTO's body, which purpose is to issue a final verdict on the tensions on trade issues between the WTO members. It is made up from seven judges, each of whom is elected for a 4-year term. There Appellate Body needs at least three judges to be able to pass the verdicts.

The WTO's Appellate Body crisis emerged back in the early 2010s, when the US President Barack Obama Administration in 2011 and 2016 has blocked the appointment and reappointment of the Appellate Body members claiming the WTO has failed to protect American interests. However, since 2016, the US President Donald Trump Administration has been blocking all the appointments of the Appellate Body members. Thus, by the 10th of December, 2019, two out of its three remaining members' four-year terms came to an end, and the body was left powerless. The US Trade Representative in its "Report on the Appellate Body of the World Trade Organisation" issued on the 11th of February, 2020 claims that "the Appellate Body chronically violates the rules imposed by WTO members, undermining the dispute settlement system and the WTO generally". In particular, it claims that: