Секция «Государственное регулирование и контроль»

К проблеме кибербезопасности в условиях цифровизации государственного управления РФ

Научный руководитель – Суптело Наталья Петровна

Бондарев Александр Владимирович
Студент (бакалавр)
Московский университет имени С.Ю. Витте, Факультет экономики и финансов, Москва, Россия
E-mail: alexbond2001@yandex.ru

Переход государственного управления на цифровую платформу поможет Российской Федерации войти в число лидеров мировой экономики, так как в большинстве передовых стран мира цифровизация государственного управления происходит достаточно медленно, развитие далеко отстаёт от официально обозначенных графиков.

Одно из главных мест в государственном управлении отводится платформенной модели - созданию инфраструктуры предоставления государственных услуг и повышения эффективности государственного управления. Платформа обеспечит снижение трансакционных издержек, повысит производительность труда, качество обслуживания и уровень удовлетворенности потребителей. В странах Европейского союза через 10 лет планируется полный переход в цифровой формат всех государственных сервисов для граждан (открытие компаний, поиск работы, запись в школу и детский сад и т.п.).

Роботизация процессов и возможности диалоговых систем позволят сократить чиновничий аппарат, снизить коррупционную составляющую и административные издержки. В Великобритании (лидер по индексу развития цифрового правительства) планируется к 2030 г. заменить 250 тыс. государственных служащих искусственным интеллектом (ИИ).

Но, несмотря на явные преимущества и плюсы, и установленный вектор в сторону трансформации государственного управления в цифровые технологии, существует большая вероятность обострения кибератак, с которыми сталкиваются периодически все страны мира, их количество отражено на рисунке 1.

Рисунок 1 - Количество кибератак в 2019-2020 годах по данным Positive Technologies (по месяцам) [1, с. 4].

С начала марта 2020 г. в мире отмечен рост вредоносной киберактивности. Были увеличены в 2 раза факты совершения фишинговых атак с целью кражи денеждых средств физических лиц и секретов компаний. Зафиксированы попытки кибернетических атак на критически важные инфраструктуры (аэропорты, электросети, порты, объекты водоснабжения и канализации, больницы с пациентами COVID-19). Даже Всемирная организация здравоохранения стала жертвой кибератак, в особенности хакеры активизировались с начала пандемии. Были установлены утечки в публичный доступ активных адресов электронных почт и паролей около 450-ти сотрудников, а также тысячи учётных записей и паролей других лиц-участников борьбы с коронавирусной угрозой. Подобной защитой серверов пользуются партнёрские компании ВОЗ [2].

9 декабря 2020 г. в Москве произошла утечка персональных данных пациентов переболевших Covid-19, в сеть попали более 350-ти файлов. Хотя руководитель департамента информационных технологий Москвы отрицает наличие взлома системы, ссылаясь на человеческий фактор, система является незащищённой, если допускает подобные инциденты.

Как отмечает бывший генерал-лейтенант МВД, ныне Президент российской секции Международной полицейской ассоциации Юрий Жданов, за период января-мая 2020 г.

общее количество преступлений в России посредством информационно-коммуникационных технологий (ИКТ) увеличилось в сравнении с тем же периодом 2019 г. на 85,1% и превысило 180 тыс, преступлений с использованием расчётных пластиковых карт - в 4,7 раз, почти 64 тыс., с использованием средств мобильной связи - в 2 раза, более 76,5 тыс. По данным Главного информационно-аналитического центра МВД РФ самый большой рост киберпреступлений фиксируется в зонах: Москвы, Санкт-Петербурга, Московской, Калининградской, Новгородской, Ростовской областях, Республиках Ингушетия, Бурятия, Башкортостан, Еврейской АО.

1 октября 2019 г. руководителем отдела киберзащиты компании Comparitech Бобом Дьяченко была обнаружена в свободном доступе на сервере Amazon Web Services Elasticsearch база налоговых деклараций граждан России за период 2009-2016 гг., которая насчитывала примерно 20 млн документов с информацией об адресе, ФИО, статусе резидентов, номере паспортов, телефонных номерах, идентификационных номерах налогоплательщиков (ИНН), именах работодателей и суммы налогов [3].

Основными жертвами кибератак становятся отрасли государственных учреждений, промышленности, медицины, сферы науки и образования, и финансовая отрасль. По мере перехода государств в цифровую систему число таких показателей будет неуклонно расти. В 14-м издании доклада Всемирного экономического форума о глобальных рисках за 2019 г. "массовое мошенничество и кража данных" занимает 4 место в рейтинге Глобальных рисков с прогнозом на 10-летний горизонт, "кибератаки" занимают 5 место. Как отмечается в докладе, киберриски укрепляют свои позиции наряду с экологическими проблемами [4, с. 16].

Вследствие обнаружения Глобальной угрозы необходимо оперативно принимать меры противодействия, пока ситуация не стала критической для экономики России и мировой экономики. На стадии внедрения цифрового государственного управления следует обеспечивать кибербезопасность для её пользователей и попавших в сеть данных. В декабре 2019 г. Генеральной Ассамблеей ООН была принята резолюция России по разработке международной конвенции для борьбы с киберпреступлениями. Так же необходимо обеспечить:

1) Согласованные международные оперативные действия по созданию безопасного и свободного от IT-злоумышленников цифрового пространства;
2) Не стандартизировать цифровую систему, исключить аналоговые структуры цифровизации у стран мира, в связи с риском массовых кибератак по всем серверам стран мира. Стоит уделить внимание проработке индивидуальной программы перехода на цифровую модель для Отечественной цифровизации государственного управления;
3) Необходимо объединить усилия Окинавской хартии глобального информационного общества по ликвидации очагов активности киберпреступлений;
4) Своевременно проверять системы на уязвимые места, в особенности уже подвергавшиеся атакам извне;
5) Осуществлять мониторинг сетей и при возникновении угрозы моментально изолировать систему от внешних соединений;
6) Особое внимание уделять съёмным носителям и самим ПК в государственном аппарате при работе с системой.

Безусловно человечество находится на стадии огромных перемен, наступил век компьютерных технологий и вопрос полной цифровизации управления и экономики давно назрел. С появлением компьютера был проложен путь к постепенному перемещению баз данных в цифровую среду. Череда сокращений целых секторов экономики и рабочих мест в связи с

цифровизацией неизбежна, но необходимость перехода обозначилась текущей обстановкой с COVID-19, когда многие компании, госуправление, муниципальные учреждения и т. д. были вынуждены функционировать удалённо. Но нельзя игнорировать риски киберпандемии, важнейшим шагом к её избежанию будет доскональная проработка и укрепление плана цифровой трансформации для России (для нашей страны).

Источники и литература

1) Аналитическая статья компании Positive Technologies: "Актуальные киберугрозы: III квартал 2020 года" [Электронный ресурс]. - URL: https://clck.ru/TV3zB
2) Всемирная организация здравоохранения: "О пятикратном увеличении количества кибератак и призывает к бдительности" [Электронный ресурс], режим электронного доступа, URL: https://www.who.int/ru/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
3) Статья журнала Forbes "Данные 20 млн россиян год лежали в открытом доступе" [Электронный ресурс], режим электронного доступа, URL: https://clck.ru/RVyyK
4) The Global Risks Report 2019 //14th Edition [Электронный ресурс]. URL: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Иллюстрации

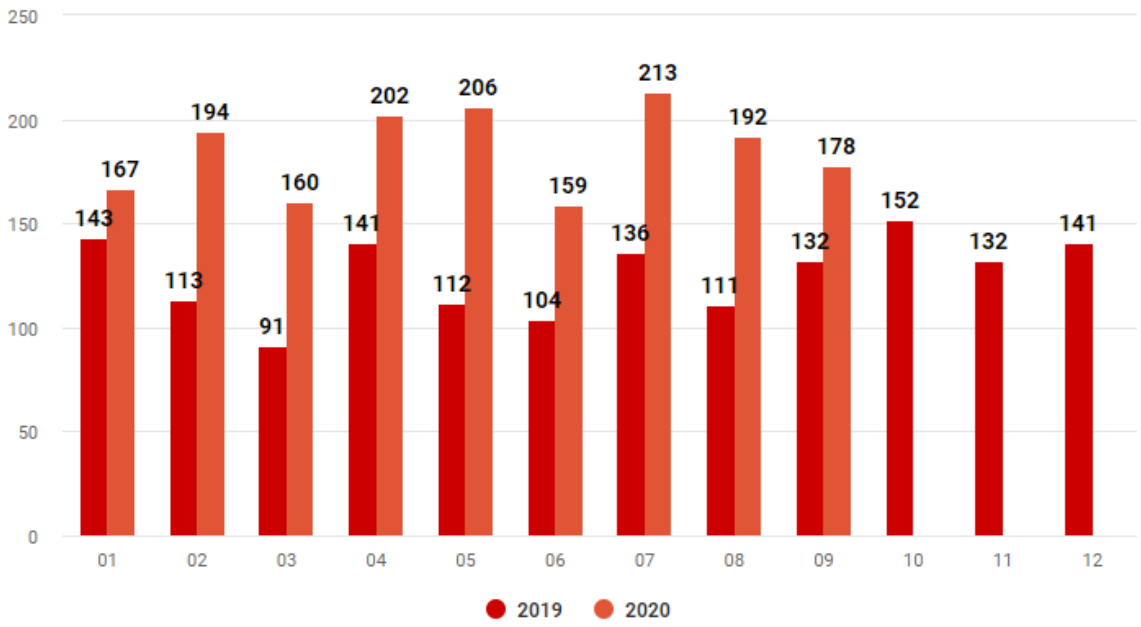

Рис. 1. Количество кибератак в 2019-2020 годах по данным Positive Technologies (по месяцам)