

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://stuservis.ru/nauchnaya-statya/243686>

Тип работы: Научная статья

Предмет: Информационные технологии

-

Аннотация: Отмечена важность поддержания стабильного функционирования ГИС в условиях пандемии, актуальность проблемы информационной безопасности обусловлена синергетическим эффектом, проанализированы случаи сбоев государственных сервисов на примере российских и зарубежных информационных ресурсов, определены тенденции дальнейшего развития в обеспечении информационной безопасности работы ГИС.

Ключевые слова: Информационная безопасность, государственная информационная система, коронавирус, кибербезопасность, COVID-19.

Введение

Очередным вызовом для мирового сообщества сегодня, стала вспышка коронавирусной инфекции (COVID-19). Данный вирус оказал влияние не только на сферу здравоохранения, но и стал триггером к масштабной цифро-визации, запустив процесс адаптации всех сфер жизни общества к условиям новой «дистанционной» реальности. Все это привело к трансформации способов и видов взаимодействия между органами государственной власти и гражданами, реализуемой посредством интеграции все большего количества государственных институтов в цифровое пространство. Работа государственных информационных систем осуществляется путем создания новых автоматизированных процессов сбора и обработки информации, необходимой для реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях, а также повышения эффективности обмена информацией и прогноза ее развития [1; 6].

Основная часть

Введение ограничительных мер в связи с распространением COVID-19 сделало затруднительным оказание государственных и муниципальных услуг посредством физического обращения граждан в офис соответствующей службы. В таких условиях ГИС стали ключом к поддержанию оказываемых гражданам услуг на должном уровне. Таким образом, государственные информационные системы являются необходимой составляющей для обеспечения стабильного функционирования государственной инфраструктуры в условиях пандемии. Следовательно, особого внимания заслуживает обеспечение информационной безопасности ГИС, так как даже кратковременная дестабилизация процесса взаимодействия между государством и гражданами, может привести к потере социальной и, возможно, экономической стабильности страны.

Так, например, официальный портал мэра Москвы и столичного правительства «mos.ru» в первый же день оформления электронных пропусков для передвижения по городу на транспорте работал с перебоями. По данным российской компании «Group IB», занимающейся детектированием и предотвращением кибератак, перебои были связаны не только с повышенным пользовательским спросом на услуги, оказываемые посредством данного ресурса, но и с участвовавшими кибератаками [7]. Генеральный директор Group IB, Илья Сачков, заявил, что на государственные цифровые сервисы Москвы было совершено несколько DDoS-атак. Сбои под воздействием кибератак свидетельствуют о несовершенстве безопасности сервиса по выдаче пропусков, поскольку он создавался в условиях ограниченности по времени [5]. Поэтому, по словам технического директора Qrator Labs Артема Гавриченко, «логично было бы полностью исключить хранение данных о гражданах и их маршрутах на серверах, обеспечив хранение информации только в зашифрованном (преобразованном) виде», дабы предотвратить компрометацию персональных данных жителей Москвы [8].

Также в условиях повышенной нагрузки опасность представляет использование устаревших технологий при работе с ГИС. Ярким примером являются США. В условиях пандемии они приняли решение реализовать социальную программу по поддержке граждан и экономики, подразумевающий денежные выплаты. Процедура получения выплат проста: нужно было оставить заявление на сайте налогового управления США (Internal Revenue Service, IRS)

1. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: Постановление Правительства РФ N 1119 от 01.11.2020 –[Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356.
2. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»: Приказ ФСТЭК России N 17 от 11 февраля 2021 г. – [Электронный ресурс]. – Режим доступа: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2021-g-n-17>.
3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: (утв. зам. директора ФСТЭК России 14 февраля 2021 г.). – [Электронный ресурс]. – Режим доступа: <https://fstec.ru/component/attachments/download/290>.
4. Госуслуги во время пандемии: на чем обожглись власти некоторых стран и как не повторить их ошибки – [Электронный ресурс]. – Режим доступа: https://www.cnews.ru/articles/2020-04-28_gosuslugi_vo_vremya_pandemii_na_chem.
5. Компанию Group-IB привлекли к расследованию кибератак на электронные сервисы Москвы – [Электронный ресурс]. – Режим доступа: <https://www.m24.ru/news/gorod/13042020/114050>.
6. «Построение системы защиты информации государственной информационной системы с применением международных стандартов» / Д. Г. Макарова, А. А. Старикова, У. В. Таратынова // Интерэкспо Гео-Сибирь. – 2020.
7. Сайт мэрии Москвы не выдержал нагрузки в первый день оформления пропусков – [Электронный ресурс]. – Режим доступа: <https://www.forbes.ru/newsroom/obshchestvo/397739-sayt-merii-moskvy-ne-vyderzhal-nagruzki-v-pervyy-den-oformleniya>.
8. Электронные пропуска не прошли проверку – [Электронный ресурс]. – Режим доступа: <https://www.kommersant.ru/doc/4321265>.
9. Check Point: число «коронавирусных» кибератак выросло до 5000 в день – [Электронный ресурс]. – Режим доступа: <https://xakep.ru/2020/04/03/coivd-19-cyberattacks>
10. Cyber Security: Innovation and Cooperation – [Электронный ресурс]. – Режим доступа: <https://www.huawei.com/en/industry-insights/technology/digital-transformation/security>.

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://stuservis.ru/nauchnaya-statya/243686>