Кому: Министерству цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан

ФИО и должность автора: Зейнелкабиденов А.Р., Главный консультант Отдела цифровизации и проектного управления Управления делами Президента Республики Казахстан

Дата: 24.02.2025 г.

АНАЛИТИЧЕСКАЯ ЗАПИСКА

Тема: Важность кибергигиены в сфере государственной службы

Введение

Кибергигиена, или цифровая гигиена, представляет собой формирование полезных привычек в области кибербезопасности, направленных на предотвращение угроз и сохранение безопасности в сети. Ее можно сравнить с личной гигиеной: в обоих случаях речь идет о регулярных мерах, способствующих поддержанию здоровья и благополучия.

Цель кибергигиены — обеспечение безопасности и стабильной работы как оборудования, так и программного обеспечения, а также защита от вредоносных программ и других угроз. Регулярное соблюдение принципов цифровой гигиены помогает сохранять данные в безопасности. Подобно другим важным привычкам, такие процедуры требуют постоянного повторения для достижения эффекта.

Соблюдение кибергигиены предотвращает утечку личных данных и кражу информации киберпреступниками, а также помогает своевременно обновлять программное обеспечение и операционные системы. Актуальность этой концепции значительно возросла с началом пандемии COVID-19, когда переход на удаленную работу способствовал росту киберпреступлений.

Основная часть

Информационная безопасность в сфере государственной службы становится все более значимым, как в мировом масштабе, так и в контексте Казахстана. О том, как в целом в мире обстоят дела с компьютерной безопасностью, рассказали аналитики Finprom.kz.

В 2023 году, по данным Statista, от атак программ-вымогателей пострадало 75,7% всех мировых организаций. Их доля с каждым годом растет. Так, например, в 2018-м пострадало лишь 55,1% организаций, в 2019-м — 56,1%, в 2020-м — 62,4%, в 2021-м — 68,5%, в 2022 году — 71%.

Чаще всего от атак страдают **государственный**, производственный и профессиональный секторы.

В январе 2024 года в Казахстане было зафиксировано 4,2 тыс. кибератак — сразу вдвое больше, чем годом ранее. Большая часть кибератак пришлась на заражение компьютеров вредоносными вирусами, сетевыми червями и троянами: 2,8 тыс. случаев, годовой рост — сразу на 69,1%. Количество фишинговых атак выросло сразу в 14 раз, до 594 случаев, число атак ботнетов — в 2,4 раза, до 322 случаев, количество инцидентов отсутствия доступа к интернет-ресурсу — на 2,3%, до 88 случаев. В то же время число DoS/DDoS-атак уменьшилось на 20%, до 16 случаев, а количество инцидентов несанкционированного доступа и модификации содержания — до всего 5 случаев, против 93 случаев годом ранее.

Наиболее часто жертвами киберпреступлений в Казахстане в 2023 и 2024 годах становились СМИ (19%), **госучреждения (12%)**, финансовые организации (12%) и телекоммуникации (7%).

Учитывая вышеперечисленную статистику, вопрос кибербезопасности становится все более актуальным. Атаки становятся все более сложными и разнообразными, затрагивая различные сферы, включая инфраструктуру, финансовый сектор, здравоохранение и **государственные структуры**. В этой связи **кибергигиена** приобретает ключевое значение, особенно для государственных служащих. Необходимо чтобы они соблюдали строгие протоколы безопасности, чтобы минимизировать риски утечек данных, взломов и других угроз. Регулярное обновление паролей, использование многофакторной аутентификации и осведомленность о новых типах угроз — это лишь некоторые из мер, которые помогают защищать не только личные данные, но и безопасность на государственном уровне. В условиях увеличения киберугроз важно, чтобы государственные служащие знали, как правильно защищать информацию, так как последствия халатности могут быть опасным как для отдельных граждан, так и для всей страны в целом.

Международный опыт кибергигиены в сфере государственной службы

Международный опыт кибергигиены в сфере государственной службы активно развивается, и многие страны внедряют передовые практики и стандарты для защиты государственных данных, а также для обучения государственных служащих безопасному поведению в цифровом пространстве. Например, в США кибергигиена является важной частью общей стратегии национальной кибербезопасности. Здесь ключевым инструментом является Национальный институт стандартов и технологий (NIST), который разрабатывает стандарты и лучшие практики в области кибербезопасности, включая рекомендации по цифровой гигиене. Важно регулярно обновлять ПО, использовать многофакторную аутентификацию и обучать сотрудников основам кибербезопасности, что является неотъемлемой частью работы государственных структур. Эстония, в свою очередь, является мировым лидером в области кибербезопасности, активно применяя передовые методы кибергигиены в государственной службе. Все госслужащие в Эстонии проходят регулярное обучение по кибербезопасности, а страна внедрила уникальную систему электронного правительства, где безопасность данных и цифровая гигиена играют ключевую роль. Кроме того, Эстония организует обучение по защите от фишинга, вредоносных программ и других угроз, что способствует высокому уровню цифровой грамотности среди государственных служащих.

Выводы и рекомендации

Казахстане, как и в других странах, число кибератак и угроз в цифровом пространстве растет, что делает вопросы кибергигиены особенно важными для государственных служащих. Атаки могут угрожать не только личным данным, но и безопасности национальной информационной инфраструктуры. Стоит отметить, что в некоторых государственных структурах Республики Казахстан наблюдается нехватка системного обучения по вопросам кибербезопасности и кибергигиены, что увеличивает риски для государственных данных и процессов. Хотя в Казахстане уже разработаны и внедряются некоторые нормы и стандарты в области кибербезопасности, их внедрение и контроль на всех уровнях государственной службы остаются недостаточно эффективными.

Для обеспечения соблюдения цифровой гигиены предлагается нижеследующие рекомендации:

Первое, разработать и внедрить четкие стандарты и регламенты для государственной службы в области кибергигиены, включая правила по использованию паролей, защите информации и обновлениям программного обеспечения. Эти стандарты должны быть обязательными для всех государственных учреждений.

Второе, организация постоянных тренингов, семинаров и курсов по кибербезопасности и цифровой гигиене для госслужащих позволит повысить их осведомленность о текущих угрозах и методах защиты. Также необходимо внедрить систему сертификации по кибербезопасности.

Третье, на всех уровнях государственной службы необходимо внедрить практики многофакторной аутентификации, а также обязательное использование шифрования для защиты персональных данных и служебной информации.

Четвертое, внедрить систему мониторинга киберугроз и быстрого реагирования на инциденты. Создание специализированных подразделений в каждом государственном учреждении для выявления и устранения киберугроз позволит снизить риски утечек и атак.

Пятое, следует развивать сотрудничество с международными организациями и государствами в области кибербезопасности, перенимать лучшие практики и внедрять их в систему госслужбы.

Шестое, необходимо активно использовать передовые технологии защиты данных, такие как блокчейн для обеспечения прозрачности и безопасности информации, а также искусственный интеллект для обнаружения аномальной активности в сетях государственных структур

Эти меры помогут значительно повысить уровень кибербезопасности и предотвратить угрозы в области цифровой гигиены для государственных служащих в Республике Казахстан.

Список использованных источников

Число кибератак растет в Казахстане (2024). https://profit.kz/news

Хакеры атакуют: количество кибератак в РК выросло вдвое (2024). https://finprom.kz/ru/article/hakery-atakuyut-kolichestvo-kiberatak-v-rk-vyroslo-vdvoe

Цифровая гигиена поможет обеспечить безопасность в сети (2024). https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-hygiene-habits