УДК 004

Николаев Ю.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Байрушин Ф.Т.
Уфимский университет науки и технологий, Уфа

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ МУНИЦИПАЛЬНЫХ УЧРЕЖДЕНИЙ

Аннотация. В статье рассматриваются ключевые угрозы информационной безопасности в государственных муниципальных учреждениях, включая фишинг, вредоносное ПО и человеческий фактор. Приводятся примеры угроз, представляющих опасность для государственных и муниципальных органов. Предложены меры устранения угроз информационной безопасности: обучение сотрудников, переход на отечественное ПО и усиление нормативной базы.

Ключевые слова: информационная безопасность, муниципальные учреждения, фишинг, программы-вымогатели, человеческий фактор, кибератаки, цифровая гигиена, импортозамещение, защита данных.

Государственные муниципальные учреждения становятся ключевой мишенью для киберпреступников из-за концентрации конфиденциальных данных и недостаточной готовности к современным угрозам. По данным аналитиков, на госсектор приходится 15 % успешных кибератак в России, при этом 66 % утечек данных происходят по вине сотрудников. В статье анализируются основные угрозы и предлагаются меры по укреплению защиты [1].

Рассмотрим основные угрозы информационной безопасности:

1. Фишинговые атаки и социальная инженерия. Данные атака направлены на кражу или повреждение данных. Злоумышленники активно используют методы социальной инженерии, маскируясь под официальные запросы. За этим следуют утечки данных в которых личные данные сливаются в общий доступ или к необратимому повреждению этих данных. В 2024 г. 57 % атак были направлены на сотрудников через:

- СМС с ссылками на фальшивые порталы;
- фишинговые формы сбора персональных данных;

Например, в г. Уфа зафиксирован случай утечки данных через поддельный запрос в соцсетях от имени администрации города [2].

2. Вредоносное ПО и программы-вымогатели. Вредоносное ПО является одной из угроз для безопасности госучреждений. Программа-вымогатель, Spyware и прочие программы которые могут украсть данные, шпионить за пользователем, забрать контроль над ПО у госслужащего,

DDoS-S атаки и блокировка работы всех систем. Атаки с использованием шифровальщиков выросли на 23 % за 2024 г. Муниципальные учреждения уязвимы из-за:

- устаревшего ПО (40 % систем не обновляются регулярно);
- отсутствия резервного копирования данных.

Каждая третья атака на госучреждения приводит к простою систем на 6+ часов [3].

3. Человеческий фактор. Человеческий фактор является основной проблемой утечки или потери информации. Основной она является в силу того, что остальные проблемы исходят именно из-за человека, так как он является главной из угроз для сохранности ПО. Загрузка вредоносного ПО, неспособность организовать грамотную программу для борьбы с кибератаками, практические ошибки в работе с ПО, приводящие к потере информации, и заинтересованность конкретного работника в потере информации. На это указывает статистика - 66 % инцидентов связаны с ошибками персонала:

- передача логинов и паролей третьим лицам;
- использование личных устройств для работы.

Таблица 1

Статистика угроз (2024 г.)

Показатель	Значение
Успешные атаки на госсектор	15 %
Утечки из-за человеческого фактора	66 %
Внедрение отечественных решений	37 %

Рис. 1. Распределение типов кибератак на муниципальные учреждения

Рассмотрим рекомендации по защите от угроз информационной безопасности:

1. Обучение сотрудников. В рамках борьбы с кибератаками обучение сотрудников и отсев «ненадежных» сотрудников является самым важным делом, в т. ч.:

• внедрение программ по цифровой гигиене (ежеквартальные тренинги);

2. Технические меры:

• переход на отечественное ПО (37 % учреждений уже используют российские программы);

• регулярное обновление систем;

• внедрение нейросетей с обучением сотрудников для работы с этой технологией.

3. Нормативное регулирование. Нормативная база является важным формальным механизмом закрепления основ борьбы с кибератаками, признавая их существование дарованием им определенного статуса и определяя права и обязанности сотрудников по борьбе с киберугрозами. Для этого необходимо:

• разработка стандартов безопасности для муниципальных ИС;

• создание единого центра мониторинга угроз

Например, в Республике Башкортостан внедрена система анализа уязвимостей, снизившая число успешных атак на 18 %. [4]

Таким образом, защита данных в муниципальных учреждениях требует комплексного подхода: сочетания технологий, обучения и нормативной базы. Приоритетными задачами остаются борьба с человеческим фактором и импортозамещение. Как показала практика, учреждения, внедрившие программы цифровой гигиены, сокращают риски утечек информации на 40 %.

Список использованных источников:

1. Попкова А.А. Парфенов К.В. Алборов А.Р. Угрозы информационной безопасности в государственном секторе России // Известия высших учебных заведений. Социология. Экономика. Политика. 2024. С. 77–92. Электрон. версия. URL: https://cyberleninka.ru/article/n/ugrozy-informatsionnoy-bezopasnosti-v-gosudarstvennom-sektore-rossii.

2. Как учитывать отечественное программное обеспечение. URL: https://cfo.bashkortostan.ru/presscenter/news/658844/.

3. Цифра дня: подсчитано количество всех кибератак на Россию за 2024 г. URL: https://hi-tech.mail.ru/news/121003-cifra-dnya-podschitano-kolichestvo-vseh-kiberatak-na-rossiyu-za-2024-god/.

4. Капкова В.А. Информационная безопасность в системе государственной и муниципальной службы // Молодой ученый. 2023. № 47 (494). С. 96–99. URL: https://moluch.ru/archive/494/107989/.

Nikolaev Y.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Bayrushin F.T.
Ufa University of Science and Technology, Ufa

THREATS TO INFORMATION SECURITY OF STATE MUNICIPAL INSTITUTIONS

Abstract. The article discusses the key threats to information security in government and municipal institutions, including phishing, malware, and the human factor. Examples of threats that pose a danger to government and municipal bodies are provided. Measures to eliminate information security threats are proposed: staff training, switching to domestic software, and strengthening the regulatory framework.

Keywords: information security, municipal institutions, phishing, ransomware, human factor, cyberattacks, digital hygiene, import substitution, data protection.