

СЛУЖЕБНАЯ ЗАПИСКА

Начальнику службы
информационных технологий,
автоматизации и связи

25. 06.2025 № 207

М.Т. Сабыров

Об уязвимостях

Уважаемый Максат Тилекович!

В рамках плановых мероприятий по обеспечению информационной безопасности и оценки защищенности компонентов ИТ-инфраструктуры было выполнено сканирование с использованием системы «MaxPatrol 8», в результате которого были выявлены уязвимости.

В зоне DMZ были выявлены следующие уязвимости:

- **gazprom.kg** — 5 уязвимостей
- **Vtiger CRM** — 144 уязвимости
- **Oktell** — 6 уязвимостей
- **api.gazprom.kg** — 6 уязвимостей

В Production-зоне по результатам сканирования выявлены критические и высокоуровневые уязвимости, включая:

- Выполнение произвольных команд (CVE-2015-4642, CVSS 10.0)
- Целочисленное переполнение (CVE-2015-4643, CVSS 9.8)
- Отказ в обслуживании (CVE-2015-5589 и др.)
- Разглашение конфиденциальной информации (несколько CVE, CVSS до 9.1)
- Обход ограничений безопасности и несанкционированные действия

Наиболее уязвимыми узлами оказались:

- **Прокси сервер** — 161 уязвимость
- **Сервер МФЦ №2** — 109 уязвимостей
- **Сервер интранет портала и форм KPI и Сервер "Единое окно"** — по 99 уязвимостей

В связи с изложенным считаем необходимым:

- В кратчайшие сроки устранить выявленные уязвимости.

- Обеспечить приведение используемого программного обеспечения в соответствие с требованиями политики информационной безопасности и действующего лицензионного законодательства, включая приобретение необходимых лицензий.
- Обратить внимание на следующие критические замечания:
 - Отсутствует лицензия на операционную систему Microsoft Windows.
 - Не используется официальная лицензия для серверных операционных систем Microsoft Windows Server.
 - Отсутствует лицензия для почтового сервера Microsoft Exchange.
 - Отсутствует действующая лицензия для гипервизора VMware ESXi.
 - Также выявлено отсутствие лицензий и актуальных обновлений на ряд инфраструктурных систем, что представляет потенциальный риск для стабильности и безопасности ИТ-среды.

Следует особо отметить, что указанные выше несоответствия противоречат требованиям действующего Приказа № 92 от 24.07.2015 «Политика информационной безопасности» ОсОО «Газпром Кыргызстан», раздела 12.3 «Меры по обеспечению информационной безопасности в автоматизированных системах и вычислительных сетях», где:

- устанавливаются правила использования работниками только лицензионных продуктов, приобретаемых Обществом, и обязательства по порядку их использования и нераспространения;
- запрещается использование программного обеспечения с нарушениями лицензионных договоров.

Подробный отчет с перечислением всех уязвимостей, уровней риска и рекомендациями по устранению прилагается.

Приложение. Отчет по уязвимостям 396стр.

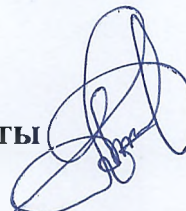
Руководитель ГИБ СКЗ



Н.У. Сарчалов

Согласовано:

**Заместитель Генерального директора -
начальник Службы корпоративной защиты**



Б.Б. Курманалиев