ПромСвязьИнвест
расчетная небанковская кредитная организация
367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»
ОКПО 43340114 БИК № 048209395 корсчет 30103810982090000039 5
тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

**«01» февраля 2021г.** **г. Махачкала**

**«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за январь 2021 г.»**

В связи с необходимостью снижения рисков воздействия вредоносного кода, рисков использования уязвимостей программного обеспечения и повышения уровня защиты информации при работе с системой дистанционного банковского обслуживания «iBank2» (Интернет-банком) служба информационной безопасности РНКО «ПРОМСВЯЗЬ ИНВЕСТ» (ООО) рекомендует it-специалистам наших клиентов (организаций и индивидуальных предпринимателей) применять в своей работе рекомендации по защите информации, указанные в Приложениях 1 и 2 к данному письму. В случае возникновения вопросов по применению рекомендаций просим Вас позвонить в службу информационной безопасности по номеру 8 (8722) 51-70-44.

**ВРИО Председателя Правления** **Исланов М.О.**

подпись

**М.П.**

**Исп. Ирганов Ю.Г.**
**Руководитель СИБ**
**8 (8722) 62-62-39**

**Приложение № 1**
**к информационному письму**
**«Информирование клиентов системы**
**дистанционного банковского**
**обслуживания «iBank2» о мерах**
**защиты за январь 2021 г.»**

По информации **ФИНЦЕРТ (центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, специального структурного подразделения Банка России)** участились случаи распространения вредоносного программного обеспечения семейства «RTM», ориентированного на клиентов кредитно-финансовых организаций, являющихся юридическими лицами и индивидуальными предпринимателями.

| | |
|---|---|
| URL-адреса и IP-адреса, рекомендуемые к блокировке it-специалистами организаций и индивидуальных предпринимателей через сетевые экраны, брандмауэры, сетевое оборудование | **94.156.35.136**<br>**77.208.157.70**<br>**45.156.26.90**<br>**206.189.15.193** |

При работе с электронной почтой организациям и индивидуальным предпринимателям следует учитывать, что участились случаи отправки по электронной почте ложных писем от мошенников. Целью данных писем является распространение вредоносного кода с целью кражи денежных средств. Подобные письма содержат файлы со следующими именами:

**Исполнительный лист 154211671.scr**
**Na oplatu ponedel'nik.exe**
**Dokumenty yanvar'.exe**
**Dokumenty 11.01.exe**
**Akt za dekabr'.exe**
**Paket dok-ov za dekabr'.exe**
**Zakryvayushchie dokumenty 11e yanvarya.exe**

При обнаружении во входящих письмах своей электронной почты писем с файлами с подобными именами не рекомендуется открывать такие файлы и такие письма.

На компьютере, с использованием которого осуществляется работа в системе ДБО «iBank2», не рекомендуется устанавливать программное обеспечение, имеющее уязвимости с критичным уровнем опасности. К такому программному обеспечению относится программное обеспечение, указанное в таблице ниже.

| № | Наименование уязвимого программного Обеспечения | Идентификатор уязвимостей | Описание уязвимости | Дата выявления | Ссылка на источники | Наличие обновлений |
|---|---|---|---|---|---|---|
| 1. | Удаленное выполнение кода в Mozilla Thunderbird | MITRE: CVE-2020-26970 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством подключения пользователя к вредоносному | 2 декабря 2020 г. | https://www.cybersecurity-help.cz/vdb/SB2020120213 | Есть |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | SMTP-серверу. Уязвимость обусловлена некорректной обработкой ответных сообщений от SMTP-сервера. | | | |
| 2. | Выполнение произвольного кода в Oracle VM VirtualBox | MITRE: CVE-2021-2074 | Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных в компоненте Core | 20 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB20210120100 https://www.oracle.com/security-alerts/cpujan2021.html https://www.oracle.com/security-alerts/cpujan2021verbose.html | Есть |
| 3. | Выполнение произвольного кода в Oracle Database Server | MITRE: CVE-2021-2035 | Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных в планировщике СУБД | 19 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021011912 https://www.oracle.com/security-alerts/cpujan2021.html https://www.oracle.com/security-alerts/cpujan2021verbose.html | Есть |
| 4. | Выполнение произвольного кода в продуктах Oracle | MITRE: CVE-2020-11984 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена ошибкой границ памяти | 8 августа 2020 г. | https://www.cybersecurity-help.cz/vdb/SB2020080806 https://www.oracle.com/security-alerts/cpujan2021.html https://www.oracle.com/security-alerts/cpujan2021verbose.html | Есть |
| 5. | Выполнение произвольного кода в Adobe Bridge CC | MITRE: CVE-2021-21013 CVE-2021-21012 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти при обработке входных данных | 12 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021011245 https://helpx.adobe.com/security/products/bridge/apsb21-07.html | Есть |
| 6. | Множественные уязвимости в маршрутизаторе D-Link DSL-2888A | MITRE: CVE-2020-24579 | Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к уязвимому устройству посредством использования IP-адреса пользователя после его успешного входа в систему на уязвимом устройстве Уязвимость обусловлена некорректной работой механизма управления сеансом, который полагается только на IP-адрес пользователя | 18 декабря 2020 г. | https://www.cybersecurity-help.cz/vdb/SB2020121803 https://www.trustwave.com/en-us/resources/security-resources/security-advisories/?fid=28241 | Есть |
| 7. | Выполнение произвольного кода в ПО Zyxel | Не определен | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке HTTP-запросов на веб-сервере zhttpd | 19 декабря 2020 г. | https://www.cybersecurity-help.cz/vdb/SB2020121920 https://www.zyxel.com/support/Zyxel-security-advisory-for-remote-code-execution-and-denial-of-service-vulnerabilities-of-CPE.shtml | Есть |
| 8. | Выполнение произвольного кода в Mozilla Firefox | MITRE: CVE-2020-16044 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой фрагмента COOKIE-ECHO в пакете SCTP | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021010608 | Есть |
| 9. | Множественные уязвимости в Google Chrome | MITRE: Не определен | Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021010701 | Есть |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректным определением границы памяти при обработке входных данных | | | |
| 10. | Множественные уязвимости в Google Chrome | MITRE: CVE-2021-21106 CVE-2021-21107 CVE-2021-21108 CVE-2021-21109 CVE-2021-21110 CVE-2021-21112 CVE-2021-21114 CVE-2021-21115 | Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректным использованием памяти в компонентах уязвимого программного обеспечения. | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021010701 | Есть |
| 11. | Множественные уязвимости в Google Chrome | MITRE: CVE-2021-21113 CVE-2021-21116 | Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой объектов в памяти приложения. | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021010701 | Есть |
| 12. | Множественные уязвимости в Google Chrome | MITRE: CVE-2020-15995 | Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой содержимого HTML-страниц. | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021010701 | Есть |
| 13. | Множественные уязвимости в Google Chrome | MITRE: CVE-2020-16043 | Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных. | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021010701 | Есть |
| 14. | Множественные уязвимости в Google Chrome | MITRE: CVE-2021-21111 | Эксплуатация уязвимости позволяет удалённому злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректной настройкой политик безопасности для веб-интерфейса приложения. | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021010701 | Есть |
| 15. | Множественные уязвимости в Mozilla Firefox | MITRE: CVE-2021-23954 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов при использовании операторов логического присваивания. | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021012626 https://www.mozilla.org/en-US/security/advisories/mfsa2021-03/ https://www.mozilla.org/en-US/security/advisories/mfsa2021-04/ | Есть |
| 16. | Множественные уязвимости в Google Chrome | MITRE: CVE-2021-21128 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021011911 https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html | Есть |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти при обработке HTML-данных. | | | |
| 17. | Множественные уязвимости в Google Chrome | MITRE: CVE-2021-21135 | Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в уязвимом приложении посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией компонента Performance API. | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021011911 https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html | Есть |
| 18. | Множественные уязвимости в Google Chrome | MITRE: CVE-2021-21117 CVE-2021-21125 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной политикой безопасности. | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021011911 https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html | Есть |
| 19. | Множественные уязвимости в Google Chrome | MITRE: CVE-2021-21119 CVE-2021-21120 CVE-2021-21121 CVE-2021-21122 CVE-2021-21124 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения. | 6 января 2021 г. | https://www.cybersecurity-help.cz/vdb/SB2021011911 https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html | Есть |