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

«02» ноября 2020г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за октябрь 2020 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 Приложении 1 к данному письму. В случае возникновения вопросов по применению рекомендаций просим Вас позвонить в службу информационной безопасности по номеру 8 (8722) 51-70-44.

Председатель Правления _____ **Абдурахманов К.А.**
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 октябрь 2020 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	**68.183.128.248** **206.166.251.189** **206.166.251.147** **91.200.102.242** **206.166.251.204** **77.208.157.70** **hxxps://yadi.sk/d/Xz0Ip4Hlxs9AoQ** **172.86.75.45** **142.93.196.20** **206.166.251.6** **142.93.120.99**

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:

Dok-y na oplatu za sentyabr'.exe
Dokumenty 9.10.2020.exe
Sverka 12e oktyabrya.exe
Требование ФНС.rar
Электронное налоговое требование №933900900233998.rar
Электронный договор денежного займа № 189887338883773.exe
Kopii dokumentov 13.10.exe
Obespechenie kontrakta za proshlyj i za etot mesyac.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.	Выполнение произвольного кода в ARC Informatique PcVue	MITRE: CVE-2020-26867	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой при обработке сериализованных данных.	12 октября 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020101206 https://ics-cert.kaspersky.com/advisories/klcert-advisories/2020/10/09/klcert-20-015-remote-code-execution-in-arc-informatique-pcvue	Есть
2.	Множественные уязвимости в контроллерах WAGO	MITRE: CVE-2020-12506	Эксплуатация уязвимости позволяет удаленному злоумышленнику изменить настройки на целевом устройстве посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе управления.	30 сентябрь 2020 г.	https://cert.vde.com/de-de/advisories/vde-2020-027 https://cert.vde.com/de-de/advisories/vde-2020-028	Есть
3.	Удаленное выполнение кода в Cisco Video Surveillance 8000 Series	MITRE: CVE-2020-3544	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети выполнить произвольный код или вызвать отказ в обслуживании целевого устройства посредством отправки специально сформированного сетевого пакета. Уязвимость обусловлена некорректной обработкой сетевых пакетов протокола Cisco Discovery Protocol.	7 октября 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cdp-rcedos-mAHR8vNx	Есть
4.	Удаленное выполнение кода в Microsoft Office Access Connectivity Engine	MITRE: CVE-2020-16957	Эксплуатация уязвимости позволяет удаленному злоумышленцику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена некорректным определением границ буфера памяти при функционировании уязвимого ПО.	13 октября 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020101368 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16957	Есть
5.	Обход авторизации в Cisco Identity Services Engine	MITRE: CVE-2020-3467	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику, обладающему привилегиями уровня Read-Only Administrator, изменить конфигурационные настройки целевой системы посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным функционированием механизма RBAC веб-интерфейса управления.	7 октября 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-auth-bypass-uJWqLTZM	Есть
6.	Подмена DLL-файлов в Cisco Webex Teams Client for Windows	MITRE: CVE-2020-3535	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством размещения специально сформированного вредоносного DLL-файла в определенном месте. Уязвимость обусловлена некорректным функционированием механизма загрузки DLL-файлов.	7 октября 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-teams-dll-drsnH5AN	Есть
7.	Удаленное выполнение кода в Mozilla Thunderbird	MITRE: CVE-2020-15683	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия	22 октября 2020 г.	https://www.mozilla.org/en-US/security/advisories/mfsa2020-47/	Есть

			пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным определением границ памяти при обработке HTML-содержимого.			
8.	Множественные уязвимости в Google Chrome	MITRE: CVE-2020-16001 CVE-2020-16002	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена некорректным функционированием медиакомпонента в Google Chrome.	21 октября 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020102102	Есть
9.	Выполнение произвольного кода в Adobe InDesign	MITRE: CVE-2020-24421	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла формата .indd. Уязвимость обусловлена ошибкой границ памяти.	21 октября 2020 г.	https://helpx.adobe.com/security/products/indesign/apsb20-66.html https://www.cybersecurity-help.cz/vdb/SB2020102120	Есть
10.	Выполнение произвольного кода в Adobe Premiere Pro	MITRE: CVE-2020-24424	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена отсутствием кавычек в пути к исполняемому файлу в нескольких службах.	21 октября 2020 г.	https://helpx.adobe.com/security/products/premiere_pro/apsb20-64.html https://www.cybersecurity-help.cz/vdb/SB2020102117	Есть
11.	Выполнение произвольного кода в Adobe Photoshop	MITRE: CVE-2020-24420	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена отсутствием кавычек в пути к исполняемому файлу в нескольких службах.	21 октября 2020 г.	https://helpx.adobe.com/security/products/photoshop/apsb20-63.html https://www.cybersecurity-help.cz/vdb/SB2020102118	Есть
12.	Удаленное выполнение кода в Microsoft Hyper-V	MITRE: CVE-2020-1047	Эксплуатация уязвимости позволяет локальному злоумышленнику повысить привилегии в целевой системе. Уязвимость обусловлена некорректной обработкой объектов в памяти на основном сервере Hyper-V.	13 октября 2020 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1047 https://nvd.nist.gov/vuln/detail/CVE-2020-1047	Есть
13.	Выполнение произвольного кода в продуктах Oracle, использующих Apache HTTP-сервер	MITRE: CVE-2020-11984	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса на веб-сервер. Уязвимость обусловлена ошибкой границ памяти в модуле od_proxy_uwsgi.	20 октября 2020 г.	https://nvd.nist.gov/vuln/detail/CVE-2020-11984 https://www.oracle.com/security-alerts/cpuoct2020.html?504207 https://www.oracle.com/security-alerts/cpuoct2020verbose.html#BGDG	Есть
14.	Несанкционированный доступ в продуктах Oracle, использующих библиотеку dom4j	MITRE: CVE-2020-10683	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к уязвимому приложению посредством отправки специально созданного вредоносного файла. Уязвимость обусловлена некорректными настройками по умолчанию.	20 октября 2020 г.	https://nvd.nist.gov/vuln/detail/CVE-2020-10683 https://www.oracle.com/security-alerts/cpuoct2020.html?504207 https://www.oracle.com/security-alerts/cpuoct2020verbose.html#BGDG	Есть