РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО)

06.07.2020 г. г. Махачкала

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за июнь 2020 г.»

В связи с необходимостью снижения рисков воздействия вредоносного кода, рисков использования уязвимостей программного обеспечения и повышения уровня безопасности при работе с системой дистанционного банковского обслуживания «iBank2» (Интернет-банком) Комитет по информационной безопасности РНКО «ПРОМСВЯЗЬИНВЕСТ» (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 Комитет по информационной безопасности по номеру 8 (8722) 51-70-44.

Председатель Правления **К.А.Абдурахманов**

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за июнь 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	**195.123.241.43** **195.123.240.92** **142.202.190.6** 142.202.188.248 142.202.188.254 142.202.188.246 **91.200.101.10** **blockchain.info** **104.16.54.3** **104.16.55.3** **api.blockcypher.com** 104.20.21.251 104.20.20.251 142.202.190.22 142.202.190.23 **185.177.59.58** 195.123.228.224 195.123.228.78 195.123.228.197 142.202.190.43 142.202.190.42 151.80.194.85 54.36.198.88 151.80.194.90 137.74.157.157 137.74.131.213 54.36.198.90 185.81.98.70 185.81.98.49 137.74.157.159 54.36.40.119 51.254.87.67 172.86.75.54 172.86.75.52 45.61.138.160 45.61.138.53

	172.105.104.213 **172.105.29.250**

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:

Proekt dogovora za etot mesyac.exe
Proekt dogovora za maj.exe
Zapolnit' dogovor 19.05.2020.exe
Vozvrat konec maya.exe
Vse dokumenty 21.05.exe
Dokumenty na vozvrat pyatnica.exe
Na oplatu iyun'.exe
Dok-ty sverka 03.06.2020.exe
Dokumenty na vozvrat chetverg.exe
Skany podpisat'.exe
Vse dok-ty za etot mesyac.exe
Obespechenie kontrakta na 09.06.exe
Zapolnit' dogovor maj-iyun'.exe
Dokumenty nachalo iyunya.exe
Akt konec proshlogo mesyaca.exe
Akt na vozvrat konec maj.exe
Rassylka na 29.06.exe
Proekt dogovora za proshlyj mesyac.exe

При обнаружении во входящих письмах своей электронной почты писем с файлами с подобными имени 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.	Microsoft SharePoint	MITRE: CVE-2019-0604	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в уязвимом приложении посредством загрузки пользователем специально созданного вредоносного пакета приложений SharePoint. Уязвимость обусловлена некорректной проверкой исходной разметки пакета приложения.	5 марта 2019 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0604 https://nvd.nist.gov/vuln/detail/CVE-2019-0604	Есть
2.	CODESYS Control Runtime System Toolkit v3.5.14.30	MITRE: CVE-2020-6081	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного сетевого пакета. Уязвимость обусловлена	6 мая 2020 г.	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1003	нет

			некорректной проверкой подлинности данных в функционале "PLC_Task".			
3.	Cisco Firepower Management Center до v6.5.0 Cisco Firepower User Agent до v2.5.0	MITRE: CVE-2020-3318 CVE-2020-3301	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ с привилегиями администратора к уязвимой части целевой системы. Уязвимость обусловлена наличием статического пароля для учетной записи с высоким уровнем привилегий.	6 мая 2020 г.	https://nvd.nist.gov/vuln/detail/CVE-2020-3318 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmcua-statered-weeCcZet	есть
4.	Zoho ManageEngine Desktop Central до v10.0.474	MITRE: CVE-2020-10189	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного сетевого пакета. Уязвимость обусловлена некорректной проверкой предоставленных пользователем данных в методе getChartImage. 6 марта 2020 г.	6 марта 2020 г.	https://nvd.nist.gov/vuln/detail/CVE-2020-10189	есть
5.	FreeBSD: 11.0, 11.1, 11.2, 11.3, 12.0, 12.1	MITRE: CVE-2020-7454	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к данным в памяти ядра или процесса natd (Network Address Translation) в целевой системе посредством отправки специально созданного вредоносного FTP-пакета. Уязвимость обусловлена граничным условием в библиотеке libalias (3) при расчете длины в FTP-пакетах.	12 мая 2020 г.	https://www.freebsd.org/security/advisories/FreeBSD-SA-20:12.libalias.asc https://www.freebsd.org/security/advisories/FreeBSD-SA-20:13.libalias.asc https://www.cybersecurity-help.cz/vdb/SB2020051273	есть
6.	Windows: 10 1709, 10 1803, 10 1809, 10 1903, 10 1909 Windows Server: 1803, 1903, 1909, 2019	MITRE: CVE-2020-1118	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально созданного вредоносного запроса по протоколу TLS до v1.2. Уязвимость обусловлена некорректной работой механизма обмена ключами в Transport Layer Security (TLS) в ОС Windows.	12 мая 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020051268 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1118	есть
7.	BIG-IP APM до v15.1.0 BIG-IP APM Client до v7.1.9	MITRE: CVE-2020-5897	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы в браузере Internet Explorer. Уязвимость обусловлена ошибкой в BIG-IP Edge Client в компоненте Windows ActiveX.	12 мая 2020 г.	https://support.f5.com/csp/article/K20346072 https://support.f5.com/csp/article/K15478554 https://www.cybersecurity-help.cz/vdb/SB2020051317	нет
8.	Palo Alto PAN-OS до v9.0.6	MITRE: CVE-2020-2014	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды ОС с привилегиями администратора в целевой системе посредством отправки специально сформированных данных в уязвимую систему. Уязвимость обусловлена некорректной проверкой входных данных на сервере управления PAN-OS.	13 мая 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020051401	есть
9.	JSON-C: включая v0.14	MITRE: CVE-2020-12762	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного	9 мая 2020 г.	https://nvd.nist.gov/vuln/detail/CVE-2020-12762 https://github.com/json-c/json-c/pull/592	нет

			JSON файла. Уязвимость обусловлена некорректной проверкой предоставленных пользователем данных в printbuf_memappend.			
10	OpenSMTPD до v6.6.4	MITRE: CVE-2020-8794	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного почтового сообщения. Уязвимость обусловлена некорректной обработкой ответов от SMTP-сервера в функции mta_io.	25 февраля 2020 г.	https://www.openwall.com/lists/oss-security/2020/02/24/5 https://nvd.nist.gov/vuln/detail/CVE-2020-8794 https://blog.trendmicro.com/trendlabs-security-intelligence/opensmtpd-vulnerability-cve-2020-8794-can-lead-to-root-privilege-escalation-and-remote-code-execution/	есть
11	Adobe Acrobat DC до v2020.006.20042	MITRE: CVE-2020-9609	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF-файла. Уязвимость обусловлена некорректным определением границ буфера памяти на основе кучи.	12 мая 2020 г.	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1031 https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	есть
12	VLC Media Player до v 3.0.9	MITRE: CVE-2020-6071	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного вредоносного mDNS-пакета. Уязвимость обусловлена отсутствием проверки рекурсии в mDNS-пакете при обработке данных в библиотеке Videolabs libmicrodns v0.1.0.	24 марта 2020 г.	https://www.videolan.org/security/sb-vlc309.html https://www.cybersecurity-help.cz/vdb/SB2020051506 https://blog.talosintelligence.com/2020/03/vuln-spotlight-videolabs-microdns.html	есть
13	EcoStruxure Operator Terminal Expert (Vijeo XD) v3.1 Service Pack 1	MITRE: CVE-2020-7493	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла или веб-страницы. Уязвимость обусловлена некорректной проверкой целостности параметров load_extension при обработке VXDZ файлов.	13 мая 2020 г.	https://www.se.com/ww/en/download/document/SEVD-2020-133-04/ https://www.zerodayinitiative.com/advisories/ZDI-20-658/	есть
14	FreeBSD: v12.1-STABLE до r360971	MITRE: CVE-2020-7454	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного сетевого пакета. Уязвимость обусловлена некорректной проверкой длины сетевого пакета в обработчике libalias.	13 мая 2020 г.	https://www.freebsd.org/security/advisories/FreeBSD-SA-20:12.libalias.asc https://nvd.nist.gov/vuln/detail/CVE-2020-7454	есть
15	Apache Camel до v3.1.0	MITRE: CVE-2020-11973 CVE-2020-11972	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных вредоносных данных в уязвимое приложение. Уязвимость обусловлена некорректной работой компонента Java в Apache Camel RabbitMQ.	17 мая 2020 г.	https://www.openwall.com/lists/oss-security/2020/05/14/8 https://www.openwall.com/lists/oss-security/2020/05/14/9 https://www.openwall.com/lists/oss-security/2020/05/14/10 https://camel.apache.org/security/CVE-2020-11973.html https://camel.apache.org/security/CVE-2020-11972.html https://www.cybersecurity-help.cz/vdb/SB2020051702	есть
16	Wireless 1410 Gateway: от v4.6.43 до	MITRE: CVE-2020-12030	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить	17 мая 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020051517	есть

	v4.7.84		произвольные команды в уязвимом устройстве. Уязвимость обусловлена ошибкой при функционировании VLAN шлюза.			
17	PAC Project Basic до v9.6 PAC Project Professional до v9.6	CVE-2020-10612	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в уязвимом приложении. Уязвимость обусловлена некорректными настройками прав доступа при взаимодействием SoftPACAgent с SoftPACMonitor через сетевой порт 22000.	17 мая 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020051516	есть
18	Bitdefender Engines до v7.84063	MITRE: CVE-2020-8100	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством сканирования ABC специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой предоставленных пользователем данных в модуле cevakrnl.rv0.	15 мая 2020 г.	https://www.bitdefender.com/support/security-advisories/incomplete-validation-detection-code-bitdefender-engines-va-8589/ https://nvd.nist.gov/vuln/detail/CVE-2020-8100	есть
19	FreeRDP до v2.0.0-rc4	MITRE: CVE-2020-11523	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных вредоносных данных. Уязвимость обусловлена целочисленным переполнением буфера памяти в libfreerdp/gdi/region.c.	15 мая 2020 г.	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4qrh-8cp8-4x42 https://nvd.nist.gov/vuln/detail/CVE-2020-11523 https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-cgw8-3mp2-p5qw https://nvd.nist.gov/vuln/detail/CVE-2020-11524 https://www.cybersecurity-help.cz/vdb/SB2020051817	есть
20	Zulip Server до v1.5.1	Не определен	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику обойти установленные ограничения безопасности и получить несанкционированный доступ к приложению. Уязвимость обусловлена некорректными правами доступа в разрешении "Invite_by_admins_only".	17 мая 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020051909	есть
21	Nitro Pro до v13.9.1.155	MITRE: CVE-2020-6074	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF файла. Уязвимость обусловлена ошибкой использования памяти после освобождения при обработке PDF файлов.	18 мая 2020 г.	https://talosintelligence.com/vulnerability_reports/TALOS-2020-0997 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1013	есть
22	Windows: 7, 8.1, 10, 10 1607, 10 1709, 10 1803, 10 1809, 10 1903, 10 1909, RT 8.1 Windows Server: 1803, 1903, 1909, 2008, 2008 R2, 2012, 2012 R2, 2016, 2019	MITRE: CVE-2020-1048	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством запуска специально сформированного вредоносного файла. Уязвимость обусловлена некорректной работой службы диспетчера очереди печати Windows.	12 мая 2020 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1048	есть
23	Cisco Unified CCX до v12.0(1)ES03	MITRE: CVE-2020-3280	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код на целевом устройстве посредством отправки специально сформированного вредоносного пакета с	20 мая 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-rce-GMSC6RKN	есть

			сериализованным объектом java. Уязвимость обусловлена недостаточной проверкой предоставленных пользователем данных в интерфейсе удаленного управления Java.			
24	Zoho ManageEngine ServiceDesk Plus до v11.1 сборка 11115	Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в целевой системе. Уязвимость обусловлена некорректной реализацией механизма аутентификации по протоколу OAuth.	19 мая 2020 г.	https://www.manageengine.com/products/service-desk/on-premises/readme.html?112233 https://www.cybersecurity-help.cz/vdb/SB2020052027	есть
25	BIND v9.11.19, v9.14.12, v9.16.3	MITRE: CVE-2020-8616	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системе посредством отправки специально сформированного вредоносного сообщения. Уязвимость обусловлена отсутствием ограничений при обработке реферальных ссылок DNS сервером.	19 мая 2020 г.	https://www.openwall.com/lists/oss-security/2020/05/19/4 https://kb.isc.org/docs/cve-2020-8616 https://kb.isc.org/docs/cve-2020-8617 https://www.cybersecurity-help.cz/vdb/SB2020052016	есть
26	Syft до v0.2.3.a1	Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена недостаточной проверкой предоставленных пользователем данных в функции eval.	12 мая 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020052122 https://snyk.io/vuln/SNYK-PYTHON-SYFT-568873	есть
27	Dolibarr до v11.0.4	MITRE: CVE-2020-12669	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику получить НСД к данным в целевой системе посредством отправки специально сформированных вредоносных данных. Уязвимость обусловлена отсутствием проверки на корректность предоставленных данных в файле core/get_menudiv.php.	6 мая 2020 г.	https://sourceforge.net/projects/dolibarr/files/Dolibarr%20ERP-CRM/11.0.4/ https://nvd.nist.gov/vuln/detail/CVE-2020-12669	есть
28	Google Chrome до v83.0.4103.61	MITRE: CVE-2020-6465	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена отсутствием обнуления указателей на освобожденные ячейки буфера памяти в режиме чтения в Google Chrome	19 мая 2020 г.	https://chromereleases.googleblog.com/2020/05/stable-channel-update-for-desktop_19.html https://www.cybersecurity-help.cz/vdb/SB2020051918	есть
29	VMware Cloud Director до v10.1.0	MITRE: CVE-2020-3956	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	20 мая 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020052021 http://www.vmware.com/security/advisories/VMSA-2020-0010.html	есть
30	Character Animator 2020 до v3.2	MITRE: CVE-2020-9586	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена	20 мая 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020052019 https://helpx.adobe.com/security/products/character_animator/apsb20-25.html	есть

			ошибкой границ памяти.			
31	Video Insight VMS до v7.6	MITRE: CVE-2019-5997	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена недостаточной проверкой предоставленных пользователем данных.	20 мая 2020 г.	https://jvn.jp/en/jp/JVN96646182/index.html https://nvd.nist.gov/vuln/detail/CVE-2019-5997	есть
32	Cisco Prime Network Registrar: v8.3.0, v9.0, 9.1, v10.0, v10.1	MITRE: CVE-2020-3272	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально созданного вредоносного DHCP-запроса на уязвимое устройство. Уязвимость обусловлена некорректной проверкой входящего DHCP трафика.	20 мая 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020052118 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpnr-dhcp-dos-BkEZfhLP	есть
33	Cisco NX-OS на следующих продуктах: MDS 9100 Series Multilayer Fabric Switches, MDS 9250i Multiservice Fabric Switches, MDS 9300 Series Multilayer Fabric Switche.	MITRE: CVE-2020-3175	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки большого количества пакетов на интерфейс управления (mgmt0) уязвимого устройства. Уязвимость обусловлена некорректным контролем использования ресурсов.	26 февраля 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-mds-ovrld-dos	есть
34	OpenConnect v8.09	MITRE: CVE-2020-12823	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданных вредоносных данных в сертификате. Уязвимость обусловлена недостаточной проверкой предоставленных данных от удаленного сервера в функции get_cert_name в gnutls.c.	12 мая 2020 г.	https://nvd.nist.gov/vuln/detail/CVE-2020-12823 https://gitlab.com/openconnect/openconnect/-/merge_requests/108 https://bugs.gentoo.org/721570	есть
35	Whale Browser до v2.6.88.19	MITRE: CVE-2020-9753	Эксплуатация уязвимости позволяет удаленному злоумышленнику скомпрометировать целевую систему. Уязвимость обусловлена отсутствием проверки криптографической подписи установочного файла Flash в составе Whale Browser.	19 мая 2020 г.	https://cve.naver.com/detail/cve-2020-9753 https://nvd.nist.gov/vuln/detail/CVE-2020-9753	есть
36	Gitea v1.11.5	MITRE: CVE-2020-13246	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена «ошибкой блокировки» при использовании зеркала репозитория.	20 мая 2020 г.	https://github.com/go-gitea/gitea/issues/10549 https://nvd.nist.gov/vuln/detail/CVE-2020-13246	нет
37	DynamoBIM v2.5.2	MITRE: CVE-2020-7079	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного DLL файла. Уязвимость обусловлена некорректной работой механизма проверки	17 апреля 2020 г.	https://nvd.nist.gov/vuln/detail/CVE-2020-7079 https://www.autodesk.com/trust/security-advisories/adsk-sa-2020-0001	есть

			подписи при автоматической загрузке официальных пакетов Autodesk.			