НКО «МОНЕТА» (ООО) ИНН 1215192632, КПП 121501001 ОГРН 1121200000316, ОКПО 38024380	УТВЕРЖДЕНА Приказом Председателя Правления от 27.03.2024 № 109

ПАМЯТКА
ПО ЗАЩИТЕ ОТ ВРЕДОНОСНОГО КОДА
НЕБАНКОВСКОЙ КРЕДИТНОЙ ОРГАНИЗАЦИИ
«МОНЕТА» (общество с ограниченной ответственностью)

(Версия № 1.2)

Йошкар-Ола
2024

СОДЕРЖАНИЕ

1. Контроль версий документа

Версия	Дата	Изменения
Версия 1.0	05.04.2013	Исходная версия.
Версия 1.1	15.02.2016	Изменения оформления документа в соответствии с корпоративным стандартом. Функциональные изменения не вносились.
Версия 1.2	27.03.2024	Изменения оформления документа в соответствии с корпоративным стандартом. Функциональные изменения не вносились.

2. Порядок пересмотра документа

Внесение изменений в Памятку по защите от вредоносного кода (далее памятка) проводится при возникновении следующих условий:

- существенных изменений в информационной инфраструктуре или организационной структуре Небанковской кредитной организации «МОНЕТА» (общество с ограниченной ответственностью) (далее – НКО);
- выявления инцидентов информационной безопасности, способных повлиять на процессы, описанные в настоящем Порядке;
- при появлении новых требований к обеспечению безопасности конфиденциальной информации, со стороны законодательства Российской Федерации, органов исполнительной власти Российской Федерации и Банка России.

По результатам пересмотра в документ в случае необходимости вносятся соответствующие изменения.

3. Вредоносный код

Вредоносный код – компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, и приводящая к несанкционированному уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации.

Вредоносный код обычно представляется в виде компьютерных вирусов, программ «троянских коней», систем несанкционированного удаленного управления, программ шифровальщиков/программ вымогателей и других вредоносных программ.

Вариантов проникновения вредоносного кода на компьютер или мобильное устройство большое количество, наиболее распространенными являются:

- посещение мошеннических web-сайтов, сайтов двойников, web-сайтов, зараженных вредоносным кодом;
- получение фишингового сообщения, содержащего вредоносный код или ссылку на вредоносный код через электронную почту, сети Internet, систему обмена сообщениями, SMS, MMS или из социальной сети;
- просмотр или запуск файлов на съемных носителях информации, таких как флэш-накопитель, оптических дисках и других носителях, содержащих вредоносный код;
- скачивание/сохранение файлов, содержащих вредоносный код с файлообменных сайтов или систем обмена файлами;
- скачивание программ из магазинов приложений (Google Play, Apple store, RuStore и других) содержащих вредоносный код;

- не отключать антивирусное программное обеспечение и его обновление ни под каким предлогом.

Вредоносный код может содержаться практически в любых файлах, начиная с файлов приложений, плагинов к браузерам, заканчивая электронными документами и файлов мультимедиа.

4. Средства защиты от вредоносного кода

Использование лицензионных средств антивирусной защиты. Специализированные программы-антивирусы являются эффективным средством защиты от вредоносного кода, но не гарантируют 100% защиту. При выборе антивируса рекомендуется отдать предпочтение решениям, обеспечивающим комплексную защиту и включающими в себя антивирусное программное обеспечение, активные межсетевые экраны и систему оценки репутации сайтов (так называемые, решения класса Internet Security). В качестве рекомендаций по использованию антивируса предлагается:

- настроить антивирус на работу в режиме автоматического лечения файлов;
- проверять все файлы, скачанные из сети Internet или полученные на съемных носителях информации, такие как флэш-накопители или оптические диски, а также регулярно (не реже, чем один раз в неделю) проводить полную антивирусную проверку;
- настроить антивирус на автоматическое обновление антивирусных баз и обеспечить ежедневное обновление;
- устанавливать пароль на отключения системы антивирусной защиты либо на деинсталляцию.

Для выбора подходящего и наиболее эффективного средства защиты рекомендуется изучить исследовательские отчеты от экспертов в области информационной безопасности.

Одним из лидеров в области антивирусной защиты информации является «Лаборатория Касперского». Ежегодно данный разработчик представляет новые решения не только в области защиты от вредоносного кода, но и обеспечения комплексной защиты информации как в домашних условиях, так и в условиях бизнеса. С точки зрения домашнего использования решения «Лаборатории Касперского» представляют собой интуитивно понятную систему, с которой в состоянии справиться обычный пользователь компьютера.

«Лаборатория Касперского», сайт - www.kaspersky.ru.

Другим отечественным производителем средств защиты от вредоносного кода является «Dr.WEB». Данная компания очень давно существует на рынке и обладает большим опытом в своей области. Одной из особенностей продуктов компании «Dr.WEB» является гибкая политика лицензирования, которая позволит подобрать для себя именно тот продукт, который необходим для решения поставленной задачи. Более того у «Dr.WEB» хорошо развита партнерская сеть, что иногда позволяет использовать продукты «Dr.WEB» абсолютно бесплатно, не нарушая лицензионных соглашений.

«Dr.WEB», сайт - www.drweb.ru.

В ситуациях, когда нет возможности использовать средство защиты от вредоносного кода, но существует потребность проверки файла на наличие вредоносного кода, можно воспользоваться сервисами вышеуказанных поставщиков антивирусной защиты или бесплатными версиями «Dr web cureit» или «Kaspersky Free», которые ежедневно публикуются с актуальными антивирусными базами.

5. Организационные меры по защите от вредоносного кода

Необходимо убедиться в правильности адресов Internet-сайтов, к которым происходит подключение и на которых есть потребность совершить покупки, т.к.

похожие/двойники адреса могут использоваться для осуществления неправомерных действий.

Официальным сайтом НКО «МОНЕТА» (ООО) является https://www.moneta.ru.

Необходимо использовать персонализированную учетную запись в операционной системе, доступа к которой более ни у кого нет. Кроме того учетная запись, с которой происходит работа в Internet, не должна обладать привилегированными правами, такими как администратор операционной системы или администратор безопасности операционной системы.

По возможности необходимо использовать системы многофакторной аутентификации – одноразовые SMS-пароли, Google Authenticator, Яндекс Ключ и прочее.

Необходимо повышать свою осведомленность в области информационной безопасности. Это поможет быть в курсе текущих событий в области информационной безопасности и возможно избежать действий, которые могут повлечь за собой заражение вредоносным кодом.