НБКИ НАЦИОНАЛЬНОЕ БЮРО КРЕДИТНЫХ ИСТОРИЙ

Рекомендации пользователям и источникам формирования кредитной истории

О мерах по защите информации, указанной в статье 4 Федерального закона от 30.12.2004 № 218-ФЗ «О кредитных историях» в целях противодействия ее неправомерному разглашению и незаконному использованию, в том числе от воздействия вредоносных кодов

Настоящие Рекомендации разработаны во исполнение требований п.2.2. Положения Банка России от 17.10.2022 № 808-П «О требованиях к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательных для лиц, оказывающих профессиональные услуги на финансовом рынке, к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона «О кредитных историях», при ее обработке, хранении и передаче сертифицированными средствами защиты, а также к сохранности информации, полученной в процессе деятельности кредитного рейтингового агентства».
Защищаемой информацией в соответствии с требованиями Федерального закона от 30.12.2004 № 218-ФЗ «О кредитных историях» является информация, указанная в статье 4 данного Федерального закона.

Риски несанкционированного доступа к защищаемой информации могут возникнуть в результате:

- утечки аутентификационной информации или ее разглашения сотрудниками субъектов взаимодействия;
- действий вредоносных кодов на устройствах, с использованием которых осуществляются действия в целях обработки, хранения и передачи защищаемой информации.

В целях предотвращения несанкционированного доступа к защищаемой информации пользователям и источникам формирования кредитной истории рекомендуется:

- Разработать и ввести в действие внутри Организации «Регламент предоставления, изменения и закрытия доступа к защищаемой информации», в котором необходимо учесть все нижеуказанные рекомендации;
- сохранять конфиденциальность и не сообщать посторонним лицам, в том числе родственникам, аутентификационную информацию (логины и пароли), а также сертификаты ключей электронной подписи и удаленного защищенного доступа, используемые при взаимодействии с АО «НБКИ»;
- использовать на устройствах, с использованием которых осуществляется информационное взаимодействие с АО «НБКИ», только лицензионное

системное и прикладное программное обеспечение, а также сертифицированные средства защиты информации, в том числе – средства защиты от вредоносных кодов (антивирусное ПО);

- обеспечивать контроль конфигурации устройства, с использованием которого осуществляется взаимодействие с АО «НБКИ»:
  - не допускать несанкционированного подключения разного рода устройств, осуществляющих передачу данных (USB-модемы, смартфоны) и неразрешенных к использованию носителей информации;
  - ограничить использование съемных носителей информации.
- обеспечить защиту устройств, с использованием которых осуществляется информационное взаимодействие с АО «НБКИ», от сбоев, повреждений любой природы;
- обеспечить регулярную установку обновлений системного и прикладного программного обеспечения, средств защиты от вредоносных кодов;
- использовать для доступа к устройствам, с использованием которых осуществляется информационное взаимодействие с АО «НБКИ», сложные пароли (не менее 8 символов с использованием цифр и латинских букв в верхнем и нижнем регистре) , а при возможности – многофакторную аутентификацию;
- направлять в АО «НБКИ» защищаемую информацию по открытым каналам связи (включая сеть Интернет) в защищенном от несанкционированного доступа виде, в том числе – с применением средств шифрования;
- ограничить круг своих сотрудников, имеющих право информационного взаимодействия с АО «НБКИ», и организовать регулярный контроль их действий;
- заключить с сотрудниками, имеющими право информационного взаимодействия с АО «НБКИ», обязательства о неразглашении получаемой ими из АО «НБКИ» информации;
- обеспечить своевременное ознакомление сотрудников, имеющих право информационного взаимодействия с АО «НБКИ», с настоящими Рекомендациями, отраслевыми и внутренними требованиями по защите информации, а также проводить регулярный контроль знания и выполнения этих требований.

Для своевременного обнаружения воздействия вредоносных кодов пользователям и источникам формирования кредитной истории рекомендуется предпринимать следующие меры:

- обеспечить на устройствах, используемых для взаимодействия с АО «НБКИ», функционирование постоянной защиты от вредоносных кодов в автоматическом режиме, использование средств централизованного контроля и управления средствами защиты, а также автоматическое обновление средств защиты информации от вредоносных кодов и сигнатурных баз данных;
- обеспечить проведение регулярной проверки устройств, применяемых для взаимодействия с АО «НБКИ», и используемых на них съемных носителей информации на отсутствие вредоносных кодов;
- регулярный контроль целостности и работоспособности средств защиты информации от вредоносных кодов;
- осуществление фильтрации вредоносных кодов во всех сообщениях электронной почты организации (применение защитных почтовых шлюзов).

- применение автоматизированных средств обобщения и анализа информации, фиксируемой в журналах протоколирования работы средств защиты информации от вредоносных кодов.
- регулярный контроль (рекомендуется не реже одного раза в месяц) состава и целостности программного обеспечения устройств, с использованием которых осуществляется информационное взаимодействие с АО «НБКИ»;
- использование устройств (с ограниченными функциональными возможностями, например, терминалов или технологии «тонкий клиент») для обеспечения взаимодействия через специально выделенный сервер, целостность системного программного обеспечения которого регулярно контролируется.
- разработка и тестирование планов по локализации средств вычислительной техники, подвергшихся воздействию вредоносных кодов, и последующему восстановлению работоспособности этих средств вычислительной техники.

При выборе средств защиты от вредоносных кодов рекомендуется отдавать предпочтение известным, хорошо зарекомендовавшим себя в течение продолжительного времени компаниям - разработчикам средств защиты от вредоносных кодов. Целесообразно предусматривать приобретение средств защиты у авторизованных партнеров компаний - разработчиков средств защиты от вредоносных кодов.

При утрате (потере, хищении) устройства, с использованием которого осуществлялось информационное взаимодействие с АО «НБКИ», или при подозрении на разглашение аутентификационной информации (логины, пароли) и (или) используемых для взаимодействия с АО «НБКИ» сертификатов электронной подписи и удаленного защищенного доступа, субъект взаимодействия должен немедленно сообщить об этом в АО «НБКИ» и самостоятельно инициировать их замену.