НБКИ НАЦИОНАЛЬНОЕ БЮРО КРЕДИТНЫХ ИСТОРИЙ

Рекомендации для субъектов 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:

- утраты (хищения или хищении) бумажного носителя, содержащего защищаемую информацию;
- утечки аутентификационной информации (логина и пароля от учетной записи, используемой в сервисе «Личный кабинет субъекта кредитной истории», а также аутентификационной информации (логина, пароля и кодов доступа) используемой в информационной системе «Госуслуги») или ее непреднамеренного разглашения;
- действий вредоносных кодов (например, вирусы, перехватчики паролей) на устройствах, с использованием которых осуществляются действия в целях обработки, хранения и передачи защищаемой информации.

В целях предотвращения несанкционированного доступа к защищаемой информации на бумажных носителях, субъектам кредитной истории рекомендуется:

- хранить бумажные носители, содержащие защищаемую информацию, в местах, исключающих свободный доступ посторонних лиц, в том числе родственников;
- соблюдать осмотрительность при их переносе, не доставать их без необходимости в публичных местах.

В целях предотвращения несанкционированного доступа к защищаемой информации субъектам кредитной истории рекомендуется принимать следующие меры:

- 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;

- сохранять конфиденциальность и не сообщать посторонним лицам, в том числе родственникам, аутентификационную информацию, а также сертификаты ключей электронной подписи, 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 средства защиты от вредоносных кодов (антивирусное ПО);
- при использовании сервисов АО «НБКИ» всегда сверять совпадает ли адрес сайта, на котором находится субъект, с адресом официального сайта АО «НБКИ» https://nbki.ru или https://person.nbki.ru;
- не использовать для информационного взаимодействия с АО «НБКИ» программное обеспечение под названием «НБКИ Онлайн», установленное из магазинов приложений в сети «Интернет».

Для своевременного обнаружения воздействия вредоносных кодов субъектам кредитной истории рекомендуется предпринимать следующие меры:

- проводить регулярную проверку устройства, на отсутствие вредоносных кодов. Также рекомендуется настроить на устройстве автоматическую проверку всех подключаемых съемных носителей информации на отсутствие вредоносных кодов и автоматическое обновление антивирусного ПО и сигнатурных баз данных;
- обеспечить защиту устройств, с использованием которых осуществляется информационное взаимодействие с АО «НБКИ», от сбоев, повреждений любой природы;
- регулярно устанавливать обновления системного и прикладного программного обеспечения.

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) субъектом кредитной истории устройства, с использованием которого осуществлялось информационное взаимодействие с АО «НБКИ», или при подозрении на разглашение аутентификационной информации (логины, пароль), необходимо в максимально короткие сроки инициировать смену пароля от учетной записи, которая используется для взаимодействия с АО «НБКИ». При подозрении на утечку сертификата электронной подписи необходимо незамедлительно проинформировать об этом факте Удостоверяющий центр, который выдал этот сертификат.