РЕКОМЕНДАЦИИ КЛИЕНТАМ
ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "БАЛТИНВЕСТ УК"
ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ КОДОВ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ

1. Общие положения

Настоящие рекомендаций по защите информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям, разработаны Обществом с ограниченной ответственностью "БАЛТИНВЕСТ УК" (далее по тексту – Управляющая компания) в соответствии с требованием Указания Банка России от 20.04.2021 № 757-У "Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций".

2. Возможные риски получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

Использование средств вычислительной техники при совершении финансовых операций несет в себя риски получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций от имени клиента.

Обмениваясь информацией по сети Интернет без использования дополнительных средств защиты информации, клиент принимает на себя риски ее раскрытия перед любыми третьими лицами.

Управляющей компанией предпринимает все необходимые меры по минимизации рисков за счет использования современных механизмов обеспечения безопасности, выполнения требований законодательства, применения сертифицированных средств защиты, комплексов организационных мер, но при этом не имеет возможности гарантировать полное исключение рисков получения несанкционированного доступа или воздействия вредоносного кода на участках обработки и поступления информации, на устройствах вычислительной техники, находящихся вне его контроля.

3. Меры по предотвращению несанкционированного доступа к защищаемой информации.

На сегодняшний день существует огромное количество разнообразных способов неправомерного доступа к информации, злоумышленники постоянно совершенствуют и дополняют методы социальной инженерии и манипулирования, используют новейшие средства и технологии.

3.1. Меры, позволяющие снизить риски несанкционированного доступа к защищаемой информации:

1) Выполнение правил, установленных эксплуатационной документацией на программное обеспечение, информационные ресурсы, средства защиты информации, включая средства электронной подписи.
2) Рекомендуется исключить или затруднить доступ третьих лиц к использованию устройства, посредством которого осуществляются финансовые операции.
3) Рекомендуется исключить использование устройства, посредством которого осуществляются финансовые операции, для работы с сомнительными и развлекательными сайтами.
4) Для целей совершения финансовых операций рекомендуется ограничить набор программного обеспечения только минимально необходимым, использовать на устройстве только лицензионное, регулярно обновляемое программное обеспечение с актуальной технической поддержкой.
5) Рекомендуется не открывать вложения, полученные в электронных письмах от неизвестных отправителей.
6) Рекомендуется не осуществлять финансовые операции через открытые публичные и недоверенные сети WiFi.

3.2. Меры по контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции:

1) На устройстве, используемом для совершения финансовых операций, рекомендуется разрешать работу только с предварительной авторизацией пользователя устройства (pin-код, пароль и т.д.).
2) Не рекомендуется использовать при обычной работе административные права, позволяющие вносить изменения в конфигурацию устройства.
3) Периодически контролировать журналы событий антивирусного программного обеспечения, системные журналы, перечень установленных программ и запущенных процессов, перечень подключенных устройств.
4) При запросах дополнительных прав и разрешений любым программным обеспечением производить оценку действительной необходимости предоставления таких прав.

3.3. **Меры по своевременному обнаружению воздействия вредоносного кода:**

1) На компьютере и устройствах, используемых в целях совершения финансовых операций, рекомендуется устанавливать лицензионное антивирусное программного обеспечение, которое должно регулярно обновляться производителем.
2) Рекомендуется подвергать антивирусной проверке любую информацию, получаемую из сети Интернет или на съемных носителях.
3) Рекомендуется настроить антивирусное программное обеспечение на автоматическую полную проверку устройств на предмет наличия вредоносного программного кода не реже одного раза в неделю.
4) "Лечение" и удаление зараженных файлов должно производиться антивирусным программным обеспечением в автоматическом режиме без участия пользователя.
5) При возникновении подозрения на наличие компьютерного вируса, рекомендуется провести дополнительные проверки и приостановить работу с финансовой информацией до устранения проблем.
6) В случае обнаружения антивирусным программным обеспечением вредоносного кода, рекомендуется проконтролировать отсутствие несанкционированных действий и, по возможности, произвести замену используемой в целях совершения финансовой операции аутентификационной информации.