БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ОНЛАЙН-СЕРВИСОВ АО «РЕЕСТР»

Выполнение настоящих рекомендаций по информационной безопасности позволит обеспечить защиту информационного обмена и минимизировать риски возможных потерь в случае возникновения инцидента, связанного с несанкционированным доступом к защищаемой информации.

Рекомендации по физической безопасности устройств и носителей

Исключите возможность физического доступа посторонних лиц к компьютеру или устройству с которого Вы осуществляете работу.

Настройте блокировку экрана, чтобы посторонние не могли использовать устройство или стереть с него все данные. Лучше всего настроить автоматическую блокировку с использованием пароля.

В случае кражи/утери устройства рекомендуется сменить пароли на всех аккаунтах. Также для минимизации риска получения несанкционированного доступа к информации рекомендуется применять средства шифрования для защиты чувствительной информации и использовать двухфакторную аутентификацию, если такая функция поддерживается.

Рекомендации по работе с программным обеспечением

Скачивайте и устанавливайте приложения только из официальных источников, таких как Google Play и App Store для мобильных устройств и официальных сайтов разработчиков ПО для компьютеров.

Внимательно читайте, какие доступы, разрешения и функции требует включить установленное приложение. Часто злоумышленники встраивают вредоносное ПО в клоны популярных платных приложений. Попадая в устройство, вирус эксплуатирует уязвимости старых версий ОС с целью получения повышенного контроля в системе.

Своевременно устанавливайте обновления для операционной системы, браузеров и прикладного ПО. Практика показывает, что 99% атак направлены на уязвимости, для которых разработчики выпускали обновления.

Не используйте устройства, прошедшие процедуру Jailbreak (iOS) или получения Root-прав (Android) – таким образом вы понижаете общую безопасность устройства, предусмотренную разработчиками ОС. Аналогично для устройств под управлением Windows не используйте активаторы (KMSAuto Net и пр.) Используйте только лицензионное программного обеспечение.

Перед тем как вводить логин и пароль нужно проверить, защищено ли соединение. Если перед адресами сайта Вы увидите префикс https (где «s» означает secure — безопасное), то все в порядке.

Рекомендации по защите информации от воздействия вредоносного кода

На Вашем устройстве должно быть установлено лицензированное антивирусное программное обеспечение. Рекомендуется настроить максимальной уровень безопасности политик на Вашем антивирусе, а также регулярно следить за обновлением базы антивируса.

Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка устройства на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного ПО.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа ПО, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т.п.) или нарушения работоспособности компьютера необходимо осуществить внеплановую проверка на наличие вредоносного ПО. После удаления вирусов и восстановления работоспособности компьютера необходимо произвести смену паролей на новые, удовлетворяющие требованиям рекомендаций по парольной защите.

Не открывать подозрительные письма. К ним относят письма пришедшие из неизвестного источника. Особое внимание стоит обращать на письма, отправленные из официальных инстанций и организаций: банков, налоговой, онлайн-магазинов, бюро путешествий, авиакомпаний и так далее.

Никогда сразу не переходите по ссылкам в таких письмах. Внимательно проверяйте ссылку, по которой собираетесь кликнуть: не перепутаны ли буквы в названии сайта. Если с написанием что-то не так, это верный признак, что мошенники подсовывают Вам поддельную страницу.

Не открывайте вложения от незнакомых адресатов, особенно это касается офисных документов и исполняемых файлов (с расширениями .exe, .bat и др.)

Рекомендации по парольной защите

Используйте как можно более разнообразные символы (так Ваш пароль будет менее предсказуем, а значит более надёжным). Пароль должен быть длинным – чем длиннее, тем лучше (минимально рекомендуемая длина 8 символов).

Не используйте один и тот же пароль на всех аккаунтах, рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем. Всего одна утечка паролей – и все Ваши аккаунты будут под угрозой

Не записывайте пароли, никому не передавайте и не разглашайте их. Используйте специализированные менеджеры для хранения паролей, например, KeePass Password Safe. Для аутентификации на устройствах используйте индивидуальный пароль.

Настоящие рекомендации представлены в соответствии с п.1.13 «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» (утв. Банком России 20.04.2021 № 757-П) и носят информативный характер