НФО Технологии

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ ПРОГРАММНЫХ КОДОВ, ПРИВОДЯЩИХ К НАРУШЕНИЮ ШТАТНОГО ФУНКЦИОНИРОВАНИЯ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ

г. Москва

2024 г.

Оглавление

Перечень сокращений

АВПО – антивирусное программное обеспечение;

АРМ – автоматизированное рабочее место;

АС – автоматизированная система;

ИР – информационный ресурс;

НСД – несанкционированный доступ;

ОС – операционная система;

ПО – программное обеспечение;

ППО – прикладное ПО;

ЭП – электронная подпись;

Интернет – информационно - телекоммуникационная сеть «Интернет».

ЛВС – линия высокоскоростной связи

1. Общие положения:

- Рекомендации по защите информации при проведении финансовых операций разработаны в соответствии с требованиями Положения Банка России от 20.04.2021 N 757-П "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".
- Настоящие Рекомендации подготовлены в целях защиты информации от воздействия программных кодов, возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а так же мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.
- Настоящие Рекомендации по защите информации при проведении финансовых операций входят в состав документов по обеспечению информационной безопасности и дополняют положения «Политики информационной безопасности» Общества с ограниченной ответственностью «НФО Технологии».

2. Рекомендации при работе с персональным компьютером (АРМ, ноутбук).

- На АРМ рекомендуется устанавливать только лицензионное программное обеспечение (ПО), приобретенное Компанией и имеющее все лицензии и сертификаты от поставщика услуг, предварительно протестированное на совместимость с другим используемым системным и офисным ПО.
- На АРМ рекомендуется своевременно проводить обновление ОС и ПО.
- На АРМ рекомендуется использовать лицензированное антивирусное ПО и своевременное его обновление. Антивирусное ПО на АРМ и сервере Компани рекомендуется приобретать у разных поставщиков услуг.
- Любые работы на АРМ, связанные с изменением конфигурации (программной или аппаратной), должны производиться только квалифицированными сотрудниками компании, у которых есть соответствующий допуск к работе данного типа.
- У АРМ рекомендуется блокировать USB-выходы, в которые сотрудники Компании могут бесконтрольно подключать мобильные телефоны, смартфоны, планшетные компьютеры, беспроводные (радио) интерфейсы, модемы и прочее оборудование.

- Сотрудникам Компании не рекомендуется:
    - самостоятельно устанавливать, вскрывать, разбирать, подключать персональные компьютеры, принтеры, факсы, беспроводные точки доступа, сетевое и иное дополнительное или общее оборудование;
    - самостоятельно изменять настройки сетевых интерфейсов, BIOS, устанавливать дополнительные сетевые протоколы персональных компьютеров, принтеров, факсов и иного сетевого и общего оборудования;
    - проводить любые самостоятельные действия с сетевым коммуникационным оборудованием, сетевыми розетками, патч-кордами (проводами) ЛВС;
    - самостоятельно устанавливать на компьютер дополнительные экземпляры операционных систем, создавать общедоступные сетевые ресурсы и принтеры.
- Сотрудникам Компании рекомендуется, покидая рабочее место осуществить блокировку компьютера, нажав комбинацию клавиш Ctrl+Alt+Del или Win+L далее Блокировать компьютер или выключать компьютер.
- Доступ посторонних лиц к АРМ сотрудников Компани должен быть ограничен контролируемой зоной (охранная/пропускная система защиты, СКУД).

3. Рекомендации при работе с информационно - телекоммуникационной сетью «Интернет»

- При работе в сети Интернет сотруднику Компании рекомендуется соблюдать требования российского и международного законодательства, нормы корпоративной и общей этики, требования трудовой дисциплины и внутреннего распорядка, требования по защите информации.
- При необходимости переноса в производственную сеть Компании файлов, полученных из любых внешних источников, сотруднику Компании рекомендуется самостоятельно или с помощью сотрудников службы тех. поддержки проверить файлы и носители (CD, DVD, USB) на предмет отсутствия вирусов, используя антивирусное программное обеспечение с актуальными на текущую дату антивирусными базами.
- Не рекомендуется использовать корпоративную почту для рассылки сотрудникам Компании почтовых сообщений развлекательного, рекламного и иного характера, не относящегося к выполнению должностных обязанностей.
- В случае получения по электронной почте поздравительных или иных сообщений, заведомо не относящихся к производственному процессу, данные сообщения, необходимо удалять, не открывая, т.к. они могут содержать компьютерные вирусы и иное вредоносное ПО.

4. Рекомендации по созданию, хранению и обновлению парольной защиты АРМ

- Личные пароли рекомендуется генерировать и распределять централизованно либо выбирать пользователями АС самостоятельно с учетом следующих требований:
    - длина пароля должна быть не менее 8 символов;
    - в числе символов пароля должны присутствовать символы трех категорий из числа следующих четырех:
        - ✓ прописные буквы английского алфавита от A до Z;
        - ✓ строчные буквы английского алфавита от a до z;
        - ✓ десятичные цифры (от 0 до 9);
        - ✓ неалфавитные символы (например: !, $, #, %);
    - пароль не должен включать в себя легко вычисляемые сочетания символов (например: «112», «911» и т.п.), а также общепринятые сокращения (например: «ЭВМ», «ЛВС», «USER» и т.п.);

- пароль не должен содержать имя учетной записи Пользователя или наименование его АРМ, а также какую-либо его часть;
- пароль не должен основываться на именах и датах рождения Пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о Пользователе;
- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например: «1111111», «wwwww» и т.п.);
- не может быть использована в качестве пароля комбинация символов, набираемых в закономерном порядке на клавиатуре (например, «1234567», «qwerty» и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

➢ Хранение паролей:

- не рекомендуется записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации;
- не рекомендуется сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

➢ Порядок смены паролей:

- сотрудник самостоятельно изменяет пароль доступа к учетной записи на выделенном ему компьютере;
- пароль доступа подлежит изменению каждые 3 месяца его использования;
- внеплановая полная смена паролей всех пользователей ИС должна производиться в случае прекращения полномочий (увольнение, перевод в другое структурное подразделение и другие обстоятельства) системных администраторов, администраторов информационной безопасности, которым по роду деятельности были предоставлены полномочия по управлению парольной защитой ИС Компании;

5. Рекомендации при работе и хранению носителя ключевой информации ЭП

➢ Носитель ключевой информации ЭП, содержащий ключ для аутентификации в домене, должен храниться только у его владельца. Не рекомендуется оставлять Носитель ключевой информации ЭП без присмотра, хранить в ящике рабочего стола и других, легкодоступных местах, передавать Носитель ключевой информации ЭП кому бы то ни было. Пользователь должен принять все меры для того, чтобы исключить возможность компрометации Носителя ключевой информации ЭП.

➢ Носитель ключевой информации ЭП для аутентификации в домене необходимо использовать с вводом логина и пароля. Логин и временный пароль предоставляет владелец домена. При первой аутентификации в домене необходимо заменить временный пароль на новый пароль и запомнить его. Для смены пароля необходимо руководствоваться рекомендациями по созданию парольной защиты.

➢ Носитель ключевой информации ЭП, применяемый для заверения финансово-распорядительных электронных документов, не могут быть доверяемыми.

➢ При работе с носителем ключевой информации ЭП рекомендуется использовать только лицензированные средства криптографической защиты информации.

➢ Если есть подозрения на компрометацию ключа ЭП, рекомендуется незамедлительно обратиться в Удостоверяющий цент, выпустивший ключ ЭП, для отзыва ключа ЭП.