Депозитарные и Корпоративные Технологии

Общество с ограниченной ответственностью “Депозитарные и корпоративные технологии”
Limited liability company “Depositary and corporate technologies”
ОГРН 1057746181272 ОКПО 76050006 ИНН 7729520219 КПП 771801001
Лицензия ФСФР России на осуществление депозитарной деятельности № 177-11151-000100 от 03.04.2008
Лицензия ФСФР России на осуществление деятельности специализированного депозитария инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов № 22-000-0-00098 от 02.12.2010

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

107014, г. Москва, ул. Стромынка, д. 4, корп. 1, офис 401. Тел.: (495) 641-30-31, -32, -33. Факс (495) 641-30-31. www.depotech.ru. E-mail: dkt@depotech.ru

1. Общие положения:

1.1. Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники в целях противодействия незаконным финансовым операциям (далее – Рекомендации) разработаны в соответствии с требованиями Положение Банка России от 20 апреля 2021 г. №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».

1.2. Рекомендации разработаны в целях:

- защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники в целях противодействия незаконным финансовым операциям;
- защиты от возможных рисков получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- соблюдения мер 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.

1.3. Рекомендации являются дополнением к «Политике Общества с ограниченной ответственностью «Депозитарные и корпоративные технологии» в области обеспечения безопасности информации».

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

2.1. На АРМ устанавливать только лицензионное программное обеспечение (ПО), приобретенное Обществом и имеющее все лицензии и сертификаты от поставщика услуг, предварительно протестированное на совместимость с используемым системным и прикладным ПО.

2.2. Своевременно проводить обновление операционной системы и прикладного ПО.

2.3. Использовать лицензированное антивирусное ПО и своевременно его обновлять. Антивирусное ПО на АРМ и серверах Общества рекомендуется приобретать у разных поставщиков услуг.

2.4. Любые работы на АРМ, связанные с изменением конфигурации (программной или аппаратной), должны производиться только квалифицированными работниками Общества, у которых есть соответствующий допуск к работе данного типа.

2.5. У АРМ блокировать USB-выходы, в которые работники Общества могут бесконтрольно подключать мобильные телефоны, смартфоны, планшеты, беспроводные (радио) интерфейсы, модемы и прочее оборудование.

2.6. Работникам Общества 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 и иного сетевого и общего оборудования;
- проводить любые самостоятельные действия с сетевым коммуникационным оборудованием, сетевыми розетками, патч-кордами (проводами) локальной сети;
- самостоятельно устанавливать на компьютер дополнительные экземпляры операционных систем, создавать общедоступные сетевые ресурсы.

2.7. Работникам Общества рекомендуется, покидая рабочее место, осуществить блокировку компьютера, нажав комбинацию клавиш Ctrl+Alt+Del, далее блокировать или выключить компьютер.

2.8. Доступ посторонних лиц к АРМ работников Общества должен быть ограничен.

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

3.1. При работе в сети Интернет работники Общества должны соблюдать требования российского и международного законодательства, нормы корпоративной и общей этики, требования трудовой дисциплины и внутреннего распорядка, требования по защите информации.

3.2. При необходимости переноса в вычислительную сеть Общества файлов, полученных из любых внешних источников, необходимо передать их в департамент информационных технологий с целью проверки файлов и носителей (CD, DVD, USB) на предмет отсутствия вирусов с использованием антивирусного программного обеспечения с актуальными на текущую дату антивирусными базами.

3.3. Не использовать корпоративную почту для рассылки работникам Общества почтовых сообщений развлекательного, рекламного и иного характера, не относящихся к выполнению должностных обязанностей.

3.4. В случае получения по электронной почте поздравительных или иных сообщений, 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

4.1. Личные пароли генерировать и распределять централизованно 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.).

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

4.3. Порядок смены паролей:
- пароль доступа подлежит изменению каждые 2 месяца (или ранее) его использования;
- внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, перевод в другое структурное подразделение и другие обстоятельства) системных администраторов, которым по роду деятельности были предоставлены полномочия по управлению парольной защитой.

5. Рекомендации по хранению носителя ключевой информации электронной подписи

5.1. Носитель ключевой информации электронной подписи (далее – 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.

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

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