Памятка
Правила безопасной работы на компьютере

Памятка «Правила безопасной работы на компьютере» (далее – Памятка) разработана в соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации» и другими нормативными правовыми актами Российской Федерации, регулирующими правовые отношения в области защиты информации.

Настоящая Памятка разработана в целях обеспечения соблюдения основных правил и требований по обеспечению информационной безопасности при обработке с использованием автоматизированного рабочего места (далее – АРМ) информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация).

Сотрудник, осуществляющий обработку информации и имеющий доступ к обрабатываемой защищаемой информации, содержащейся в информационных системах, является пользователем автоматизированного рабочего места (далее – Пользователь).

Обязанности Пользователя.

Пользователь обязан соблюдать требования законодательства Российской Федерации, Федеральных законов «Об информации, информационных технологиях и о защите информации», «О персональных данных», принимаемыми в соответствии с ними нормативными правовыми актами, а также требования локальных организационно-распорядительных документов в области защиты информации, принятых в организации.

Пользователь обязан:

- выполнять только те процедуры обработки информации, которые регламентированы его должностными обязанностями и правилами обработки информации;
- перед началом обработки информации, хранящейся на съемных носителях информации, необходимо осуществлять проверку данного носителя информации и файлов, размещенных на нем, на наличие компьютерных вирусов с использованием антивирусного программного обеспечения;
- соблюдать установленный режим разграничения доступа к информационным ресурсам;
- обеспечивать конфиденциальность идентификационной и парольной информации, используемой для доступа к информационным ресурсам.

Пользователю запрещается:

- записывать и хранить защищаемую информацию на неучтенных машинных носителях информации;
- оставлять носители информации без присмотра, несанкционированно передавать носители информации третьим лицам и выносить их за пределы помещений, в которых производится обработка защищаемой информации;
- отключать и изменять настройки средств антивирусной защиты;
- отключать (блокировать) и изменять настройки средств защиты информации;

- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;
- самостоятельно тиражировать или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- открывать файлы, поступившие из неизвестных внешних источников, в том числе вложенные файлы во входящие сообщения электронной почты, файлы, размещенные на съемных машинных носителях информации, файлы, загруженные из информационно-телекоммуникационной сети «Интернет», без их предварительной проверки антивирусными средствами защиты информации;
- отправлять по открытым каналам связи защищаемую информацию, которая не зашифрована сертифицированными средствами криптографической защиты информации;
- использовать для обработки или передачи защищаемой информации зарубежные почтовые и облачные сервисы (Google, Yahoo и т.п.), сервисы обмена мгновенными сообщениями, в том числе сервисы передачи голосовой и видеоинформации (ICQ, QIP, Jabber, Viber, Whatsap, Skype и т.д.), социальные сети (Twitter, Facebook, Livejournal и т.д.);
- подключать к АРМ, используемому для обработки защищаемой информации, посторонние технические средства, в том числе мобильные устройства (планшеты, смартфоны и т.п.) и неучтенные съемные машинные носители информации (флеш-накопители, usb-диски и т.п.).

Парольная защита.

При организации парольной защиты Пользователю запрещается:

- записывать и хранить свои пароли в общедоступных местах, а также в визуально легко просматриваемых (поверхность рабочего стола и его внутренние ящики, поверхность монитора ПЭВМ, на обратной стороне клавиатуры и т.д.);
- разглашать используемые идентификационные данные (относящиеся к информационным системам, средствам защиты информации, антивирусным средствам и т.п.), в том числе различные учетные данные и пароли, направлять их по открытым каналам связи, по электронной почте или сообщать посредством телефонной и иной связи;
- использовать в качестве пароля простые пароли. Например, комбинацию символов, следующих в закономерном порядке (например, 1234567, qwerty123 и т.п.), один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов, а также общеизвестные сведения о пользователе: дата рождения, имя, фамилия и т.п.;

Правила и рекомендации по обеспечению парольной защиты:

- рекомендуется осуществлять смену паролей в соответствии политикой парольной защиты в регламентированные сроки, но не реже одного раза в год;
- при смене пароля новый пароль должен отличаться от предыдущего не менее чем в 4 символах;
- не используйте простые пароли (12345, 123qwe321, 10121980 и т.п.) Пароли должны быть не менее 12 символов, содержать прописные и строчные буквы (a-z, A-Z), цифры и спецсимволы (&*!%).
- сохраняйте в тайне личный пароль;

- не используйте личные пароли (от соцсетей, личной почты и т.п.) для служебных программ и наоборот, не используйте служебные пароли для личных целей;
- никогда не сохраняйте пароли в программах или браузере;
- при временном оставлении рабочего места необходимо в обязательном порядке заблокировать компьютер (с использованием комбинации клавиш «Win+L» или «Ctrl+Alt+Del»), либо выключить компьютер.

При обнаружении фактов нарушения конфиденциальности парольной информации (компрометация парольной информации) или при возникновении подозрения, что идентификационная и парольная информация стала известна посторонним лицам, Пользователь обязан незамедлительно сообщить об этом системному администратору и (или) администратору информационной безопасности, а также произвести процедуру внеплановой смены пароля.

Внеплановая смена пароля Пользователя должна производиться в обязательном порядке в следующих случаях:

- в случае прекращения полномочий (увольнение, переход на другую работу) Пользователя;
- компрометации (подозрении на компрометацию) идентификационной и парольной информации.

Антивирусная защита.

Требования при осуществлении антивирусного контроля:

- обязательному антивирусному контролю подлежит любая информация, получаемая по каналам связи, а также данные на съемных машинных носителях информации. Контроль входящей и исходящей информации на АРМ должен осуществляться постоянно с использованием антивирусного программного обеспечения;
- всё программное обеспечение, устанавливаемое на АРМ, должно предварительно проверяться на наличие вредоносных программ;
- внеочередной антивирусный контроль всех дисков и файлов АРМ должен выполняться при обнаружении вредоносной программы или возникновения подозрения на её наличие в системе.

Обязанности пользователей при осуществлении антивирусного контроля:

- обязательная проверка на наличие вирусов используемых внешних носителей информации (диски, флеш-накопители, карты памяти и т.п.), и поступающей информации на АРМ (электронная почта и приложения к ней, скачиваемые файлы и программы из интернет, локальной вычислительной сети, и т.п.);
- немедленное обращение к системному администратору и (или) администратору информационной безопасности в случае появления подозрений на наличие вирусов;
- немедленное обращение к системному администратору и (или) администратору безопасности в случае выявления фактов, связанных со сбоями в работе средств защиты информации.

Электронная почта.

Пользователю АРМ при обработке информации с использованием электронной рабочей почты:

- не рекомендуется открывать вложенные в сообщения электронной почты файлы и документы, которые получены от неизвестных отправителей. При получении таких сообщений необходимо обратиться к системному администратору и (или) администратору информационной безопасности;
- рекомендуется всегда проверять, с какого адреса электронной почты было отправлено сообщение;
- рекомендуется при исполнении своих должностных обязанностей использовать только корпоративные сервисы электронной почты;

При организации обработки информации с использованием электронной почты Пользователю запрещается:

- использовать корпоративную электронную почту в личных целях;
- сообщать иным лицам идентификационную и парольную информацию, используемую для доступа к сервисам электронной почты и иным корпоративным информационным ресурсам;
- передавать по электронной почте, информацию ограниченного доступа (конфиденциальную информацию, персональные данные) без применения сертифицированных средств криптографической защиты информации, используемых для шифрования информации.

Ответственность пользователя.

Пользователь несет персональную ответственность за соблюдение правил и требований информационной безопасности.

Нарушение требований информационной безопасности при обработке информации на АРМ могут повлечь за собой ограничение доступа Пользователя к защищаемой информации и прекращение обработки информации на АРМ.