УТВЕРЖДАЮ
Директор ООО «Файнекс»

_____ А.А. Сташевский
20.06.2023

ПРАВИЛА
информационной безопасности при работе пользователей в информационной системе ООО «Файнекс»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила информационной безопасности при работе пользователей в информационной системе ООО «Файнекс» (далее – Правила) определяют общие требования для пользователей при работе с персональным компьютером, корпоративной электронной почтой, внешними электронными накопителями информации и использовании ресурсов сети Интернет.

1.2. Целями настоящих Правил являются повышение осведомленности пользователей в вопросах информационной безопасности ООО «Файнекс» (далее – Организация), а также снижение рисков нарушения информационной безопасности, обусловленных действиями пользователей при работе в информационной системе Организации, которые могут повлечь нарушение технологических процессов, утрату, уничтожение или разглашение конфиденциальной информации Организации.

1.3. Для целей настоящих Правил нижеприведенные термины используются в следующих значениях:

информационная безопасность (кибербезопасность), ИБ – состояние защищенности информационных активов от случайных и преднамеренных угроз, в результате реализации которых в том числе возможно нарушение свойств доступности, целостности и (или) конфиденциальности информационных активов, хищение и совершение иных противоправных действий в отношении цифровых знаков (токенов) в информационной системе Организации, перебои в работе информационной системы;

информационный ресурс Организации – информация, представленная на любом материальном носителе в форме, пригодной для ее обработки, хранения или передачи; информационные ресурсы, в том числе возникшие в результате служебной деятельности работников Организации, являются собственностью Организации; их пересылка (передача) за пределы Организации должна быть санкционирована;

информационная система Организации – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств, используемая Организацией для осуществления своей деятельности;

ЛПА – локальный правовой акт Организации;

машинные электронные накопители информации (далее – МНИ) – подключаемые к физическим портам компьютера накопители на жестких дисках, CD- и DVD-дисководы, флеш-накопители, а также иные электронные устройства, имеющие внутреннюю память;

ПК – персональный компьютер;

ПО – программное обеспечение;

пользователи – работники Организации (сторонних организаций или индивидуальные предприниматели), которым предоставлено право работы в информационной системе Организации для выполнения ими функций, предусмотренных должностными инструкциями (договорами на оказание услуг Организации);

неправомерное распространение информационных ресурсов – распространение информационных ресурсов Организации, не обусловленные требованиями государственных органов, договорами (соглашениями) с контрагентами (клиентами) Организации, платежными (информационными) технологическими процессами Организации, ЛПА, технической и иной документацией Организации;

учетные данные – имя пользователя и соответствующий ему пароль.

1.4. Иные термины, используемые в настоящих Правилах, и не указанные в пункте 1.3, имеют значения, определенные нормативными правовыми (техническими нормативными правовыми) актами Республики Беларусь, актами Наблюдательного совета Парка высоких технологий, Политикой информационной безопасности (кибербезопасности) ООО «Файнекс».

1.5. Настоящие Правила доводятся до пользователей при:

проведении вводных инструктажей пользователей при их подключении к информационной системе Организации;

проведении инструктажей в рамках процесса повышения осведомленности пользователей по вопросам ИБ;

расширения полномочий пользователей при использовании ресурсов сети Интернет, использования МНИ, ПК и корпоративной электронной почты;

проведении мероприятий в рамках реагирования на инциденты и события ИБ.

1.6. Настоящие Правила являются- обязательными для исполнения пользователями. Консультирование по вопросам, связанным с ИБ при работе в информационной системе Организации, не нашедшим отражение в настоящих Правилах, осуществляет должностное лицо, ответственному за системное администрирование и информационную безопасность.

1.7. Организацией в рамках требований законодательства Республики Беларусь и ЛПА осуществляется контроль за правильностью использования пользователями информационных ресурсов Организации, внешних информационных ресурсов, в том числе сети Интернет, предоставленных технических и программных средств, корпоративных средств коммуникаций, предоставленных прав доступа к информационным ресурсам.

1.8. В случаях, когда пересылка (копирование) пользователями

информационных ресурсов за пределы Организации имеют признаки неправомерного распространения информационных ресурсов, указанные действия могут быть временно заблокированы программно-аппаратными средствами контроля. В этих случаях должностное лицо, ответственное за системное администрирование и информационную безопасность, для проверки правомерности пересылки сведений (копирования сведений на МНИ) имеет право затребовать у пользователей объяснений, обеспечения доступа к данной информации в случае ее шифрования, в том числе посредством предоставления пользователем пароля или расшифровки в присутствии указанного должностного лица.

1.9. По фактам нарушений пользователями правил ИБ должностное лицо, ответственное за системное администрирование и информационную безопасность, осуществляет проведение служебных разбирательств в соответствии с установленными в Организации правилами.

1.10.Нарушение требований ИБ пользователями в зависимости от умысла и нанесенного ущерба Организации может повлечь применение к ним мер в соответствии с законодательством Республики Беларусь и ЛПА.

ГЛАВА 2
ОБЩИЕ ПРАВИЛА ИБ ПРИ РАБОТЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ОРГАНИЗАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ПК И УЧЕТНЫХ ДАННЫХ

2.1. Для выполнения пользователями функциональных обязанностей Организацией предоставляются ПК, а также доступ к информационным ресурсам информационной системы Организации.

2.2. Пользователи обязаны:

осуществлять доступ к информационным ресурсам информационной системы Организации только с использованием личных учетных данных;

хранить в секрете пароли личных учетных данных, никому их не передавать и не регистрировать в общедоступных местах;

не принимать и не использовать пароли чужих учетных данных;

осуществлять смену паролей с периодичностью, установленной в Организации, или при появлении сообщения, сгенерированного ПО;

не предпринимать попыток самостоятельной установки на ПК системного и прикладного ПО, их модификации, эксплуатации незадекларированных возможностей;

не предпринимать попыток несанкционированного доступа, завладения, распространения или совершения иных действий с информационными ресурсами Организации, кроме действий, предусмотренных должностными обязанностями или технологическими процессами;

не осуществлять несанкционированного фотографирования документов, в том числе с экрана монитора ПК;

не совершать действий, которые могут привести к порче или потере работоспособности ПК или иных средств автоматизации;

не допускать вскрытия корпусов ПК и иных средств автоматизации, порчи стикеров (наклеек, пломб);

блокировать работу ПК при временном оставлении рабочего места;

осуществлять выключение ПК после окончания рабочего времени (за исключением случаев, когда работа ПК в указанное время обусловлена технологическим процессом или служебной необходимостью);

осуществлять выключение ПК программным способом без механического извлечения разъема из розетки электропитания;

для разблокировки ПК, связанной с утратой пароля (истечения срока его действия), устранения сбойных и иных нештатных ситуаций, связанных с работой ПК и иных выделенных средств автоматизации, обращаться к должностному лицу, ответственному за системное администрирование и информационную безопасность.

ГЛАВА 3
ОБЩИЕ ПРАВИЛА ИБ ПРИ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ И КОРПОРАТИВНОЙ ЭЛЕКТРОННОЙ ПОЧТЫ

3.1. Использование сети Интернет обуславливает высокие риски, связанные с возможностью проникновения в информационную систему Организации вредоносных программ (кодов), нарушения технологических процессов, хищения финансовых средств, нарушения свойств безопасности информационных ресурсов.

3.2. Использование сети Интернет и корпоративной электронной почты осуществляется работниками Организации в служебных целях для:

реализации технологических процессов Организации;

обмена электронными сообщениями;

получения и распространения информации, связанной с деятельностью Организации;

информационно-аналитической работы в интересах Организации;

реализации иных служебных задач.

3.3. При использовании сети Интернет с ПК, подключенных к информационной системе Организации, запрещается:

использовать интернет-ресурсы и интернет-сервисы, в том числе внешние почтовые службы, «облачные хранилища», которые могут повлечь неконтролируемое и неправомерное распространение информационных ресурсов за пределы Организации;

создавать и использовать учетные записи в социальных сетях, размещать в Интернете информацию, имеющую отношение к деятельности Организации, за исключением случаев, когда это вызвано производственной необходимостью и регламентировано ЛПА;

загружать из сети Интернет и запускать исполняемые файлы, в том числе содержащиеся в архивах, если это не установлено соответствующими технологическими процессами Организации;

осуществлять несанкционированное использование на рабочем месте и (или) со служебного ПК внешние почтовые интернет-сервисы;

использовать прокси-сервера и анонимайзеры, размещенные в сети Интернет;

распространять угрозы, оскорбительную и порочащую других лиц информацию;

обращаться к интернет-ресурсам, содержание и тематика которых не соответствует служебным целям и задачам;

работать с сайтами при появлении сообщений интернет-браузера об угрозах ИБ;

скачивать файлы, за исключением необходимых для осуществления служебной деятельности;

осуществлять действия, направленные на получение несанкционированного доступа к ресурсам сети Интернет, модификацию и уничтожение информации, распространение вредоносного ПО;

осуществлять иные действия, которые могут нанести (обусловить) имущественный и (или) репутационный ущерб Организации.

3.4. В случае производственной необходимости допускается использование ресурсов и сервисов, указанных в подпункте 3.3 настоящих Правил, в соответствии с ЛПА о порядке использования сети Интернет.

3.5. При работе с корпоративной электронной почтой запрещается:

осуществлять несанкционированную пересылку за пределы Организации информационных ресурсов Организации;

осуществлять пересылку сведений ограниченного распространения в открытом виде; в качестве способа защиты файлов рекомендуется использование архивирования с паролем; при этом длина пароля должна составлять не менее 6 буквенно-цифровых знаков, а сам пароль должен передаваться адресату по иным каналам связи;

принимать и открывать почтовые сообщения и вложенные файлы, доставленные от неизвестного или подозрительного корреспондента; об имеющихся фактах сообщать должностному лицу, ответственному за системное администрирование и информационную безопасность;

осуществлять переписку и обмен сведениями в неслужебных целях.

ГЛАВА 4
ПРАВИЛА ИСПОЛЬЗОВАНИЯ МНИ

4.1. Использование МНИ создает повышенные риски неправомерного распространения информационных ресурсов Организации и допускается в служебных целях, предусмотренных:

требованиями государственных органов о предоставлении информации;

договорами (соглашениями) с контрагентами (клиентами) Организации;

платежными (информационными) технологическими процессами Организации;

ЛПА, технической и иной документацией Организации;

в иных случаях с разрешения непосредственного руководителя и должностного лица, ответственного за системное администрирование и информационную безопасность.

4.2. При использовании МНИ пользователи обязаны:

информацию ограниченного распространения обрабатывать на МНИ Организации, зарегистрированных у должностного лица, ответственного за системное администрирование и информационную безопасность, и имеющих соответствующую маркировку на корпусе;

за пределами Организации информацию ограниченного распространения хранить на МНИ в зашифрованном виде;

не передавать подотчетные МНИ иным лицам;

хранить МНИ, содержащие информацию ограниченного распространения, в местах, исключающих доступ к ним иных лиц;

своевременно сообщать своему непосредственному руководителю и должностному лицу, ответственного за системное администрирование и информационную безопасность, о фактах утери служебных МНИ.