

Утверждаю
Председатель Правления
КПК «Инвест»


/Р. Г. Мишустин/
«14» июня 2019 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КРЕДИТНЫЙ ПОТРЕБИТЕЛЬСКИЙ КООПЕРАТИВ «ИНВЕСТ»

Волгоград

2019 год

1. ОБЩИЕ ПОЛОЖЕНИЯ

Информация является ценным и жизненно важным ресурсом Кредитного потребительского кооператива «Инвест» (далее – Кооператив). Настоящая Политика информационной безопасности предусматривает принятие необходимых мер в целях защиты активов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Кооперативе.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник Кооператива, при этом первоочередной задачей является обеспечение безопасности всех активов Кооператива. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив Кооператива. Главные цели Кооператива не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

В настоящей Политике под термином «сотрудник» понимаются все сотрудники Кооператива. На лиц, работающих в Кооперативе по договорам гражданско-правового характера, в том числе прикомандированных, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре.

На основании заключения администратора безопасности информационных систем об определении уровня защищенности информационной системы персональных данных Кооператива и ГОСТа Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых операций. Базовый состав организационных и технических мер», в Кооперативе установлен третий минимальный уровень защиты, который соответствует 4-ому УЗПДн.

1.1. Цель и назначение настоящей Политики

Целями настоящей Политики являются:

- сохранение конфиденциальности информационных систем;
- обеспечение непрерывности доступа к информационным системам Кооператива для поддержки бизнес деятельности;
- защита целостности деловой информации с целью поддержания возможности Кооператива по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- защита персональных данных в информационных системах Кооператива;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Кооператива;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Кооперативе.

Председатель Правления Кооператива обеспечивает регулярный контроль за соблюдением положений настоящей Политики. Кроме того, проводится 1 раз в квартал периодическая проверка администратором безопасности информационных систем соблюдения информационной безопасности в Кооперативе.

1.2. Область применения настоящей Политики

Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации Кооператива. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами,

получающими доступ к информации Кооператива, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей Политики.

Кооперативу принадлежит на праве собственности вся деловая информация и вычислительные ресурсы, приобретенные (полученные) и введенные в эксплуатацию в целях осуществления ею деятельности в соответствии с действующим законодательством. Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования Кооператива, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и персонала Кооператива.

2. ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ.

2.1. Ответственность за информационные активы

В отношении всех информационных активов Кооператива определена ответственность соответствующего сотрудника Кооператива.

2.2. Контроль доступа к информационным системам

2.2.1. Общие положения

Все работы в пределах офиса Кооператива выполняются в соответствии с должностными обязанностями только на компьютерах, разрешенных к использованию в Кооперативе.

Внос в помещение Кооператива личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы Кооператива производится только при согласовании с администратором безопасности информационных систем.

Все данные (конфиденциальные или строго конфиденциальные), составляющие коммерческую тайну Кооператива и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы. Все портативные компьютеры Кооператива должны быть оснащены программным обеспечением по шифрованию жесткого диска.

Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

В процессе своей работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуются устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.

2.2.2. Доступ третьих лиц к системам Компании

Каждый сотрудник обязан немедленно уведомить администратора безопасности информационных систем обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

Доступ третьих лиц к информационным системам Кооператива должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам Кооператива должен быть четко определен, контролируем и защищен.

2.2.3. Удаленный доступ

Пользователи получают право удаленного доступа к информационным ресурсам Кооператива с учетом их взаимоотношений с Кооперативом.

Сотрудникам, использующим в работе портативные компьютеры Кооператива, может быть предоставлен удаленный доступ к сетевым ресурсам Кооператива в соответствии с правами в корпоративной информационной системе.

Сотрудникам, работающим за пределами Кооператива с использованием компьютера, не принадлежащего Кооперативу, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

Сотрудники и третьи лица, имеющие право удаленного доступа к информационным ресурсам Кооператива, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Кооператива и к каким-либо другим сетям, не принадлежащим Кооперативу.

Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Кооператива, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

2.2.4. Доступ к сети Интернет

Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила:

- сотрудникам Кооператива разрешается использовать сеть Интернет только в служебных целях;
- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;
- сотрудники Кооператива не должны использовать сеть Интернет для хранения корпоративных данных;
- работа сотрудников Кооператива с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Кооператива в сеть Интернет;
- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Кооперативу;
- сотрудники Кооператива перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть Кооператива для всех лиц, не являющихся сотрудниками Кооператива, включая членов семьи сотрудников Кооператива.

Администратор безопасности информационных систем имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

2.3. Защита оборудования

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранятся информация Кооператива.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят администратор безопасности информационных систем.

2.3.1. Аппаратное обеспечение

Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей Политики вместе именуются «компьютерное оборудование». Компьютерное оборудование, предоставленное Кооперативом, является ее собственностью и предназначено для использования исключительно в производственных целях.

Пользователи портативных компьютеров, содержащих информацию, составляющую коммерческую тайну Кооператива, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах, или обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства, в случаях, когда данный компьютер не используется.

Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности, как в офисе, так и по месту проживания. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например, в гостиницах, аэропортах, в офисах деловых партнеров и т.д., пользователи обязаны ни при каких обстоятельствах не оставлять их без присмотра.

Во время поездки в автомобиле портативный компьютер должен находиться в багажнике. На ночь его следует перенести из автомобиля в гостиничный номер.

Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима «Экранной заставки». Для установки режимов защиты пользователь должен обратиться в службу технической поддержки. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

При записи какой-либо информации на носитель для передачи его контрагентам или партнерам по бизнесу необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

Карманные персональные компьютеры, а также мобильные телефоны, имеющие функцию электронной почты и прочие переносные устройства не относятся к числу устройств, имеющих надежные механизмы защиты данных. В подобном устройстве не рекомендуется хранить конфиденциальную информацию.

2.3.2. Программное обеспечение

Все программное обеспечение, установленное на предоставленном Кооперативом компьютерном оборудовании, является собственностью Кооператива и должно использоваться исключительно в производственных целях.

Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелегальное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено администратором безопасности информационных систем Председателю Правления.

На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;
- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков;
- программное обеспечение шифрования почтовых сообщений.

Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, определяемой администратором безопасности информационных систем.

Сотрудники Кооператива не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

2.4. Правила работы с электронной почтой

Электронные сообщения (удаленные или не удаленные) могут быть доступны или получены государственными органами или конкурентами по бизнесу для их использования в качестве доказательств в процессе судебного разбирательства или при ведении бизнеса. Поэтому содержание электронных сообщений должно строго соответствовать деловой этике.

Использование электронной почты в личных целях допускается в случаях, когда получение/отправка сообщения не мешает работе других пользователей и не препятствует бизнес деятельности.

Строго конфиденциальная информация Кооператива, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

Сотрудники Кооператива для обмена документами с бизнес партнерами должны использовать адрес электронной почты Кооператива – kpk_invest@bk.ru.

Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному

получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать администратора безопасности информационных систем.

Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

Ниже перечислены недопустимые действия и случаи использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- групповая рассылка всем пользователям Кооператива сообщений/писем;
- рассылка рекламных материалов, не связанных с деятельностью Кооператива;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит корпоративным стандартам в области этики.

Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и они должны оформляться в соответствии с установленными в Кооперативе процедурами документооборота.

2.5. Сообщение об инцидентах информационной безопасности, реагирование и отчетность

Все пользователи осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте Председателю Правления и администратору безопасности информационных систем.

Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Администратор безопасности информационных систем обеспечивает контроль и учет сообщений об инцидентах и принятие соответствующих мер.

Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник Кооператива обязан:

- проинформировать администратора безопасности информационных систем;

- не подключать компьютер к сети интернет;
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети Кооператива до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором безопасности информационных систем.

2.6. Управление сетью

Администратор безопасности информационных систем контролирует содержание всех потоков данных проходящих через сеть Кооператива.

Сотрудникам Кооператива запрещается:

- нарушать информационную безопасность и работу сети Кооператива;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
- передавать информацию о сотрудниках или списки сотрудников Кооператива посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

2.6.1. Защита и сохранность данных

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях. Администратор безопасности информационных систем обязан оказывать пользователям содействие в проведении резервного копирования данных на соответствующие носители.

Ежедневно делать резервные копии всех основных служебных данных и программного обеспечения.

Только администратор безопасности информационных систем на основании заявок от руководителей подразделений может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним по согласованию с Председателем Правления.

Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

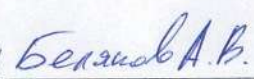
Все заявки на проведение технического обслуживания компьютеров должны направляться администратору безопасности информационных систем.

2.7. Разработка систем и управление внесением изменений

Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, согласованы Председателем Правления Кооператива и администратором безопасности информационных систем.

Политику информационной безопасности
в КПК «Инвест» разработал:
Системный администратор
(администратор безопасности
информационных систем):


(подпись)

 / Белзиков А.В. /
(расшифровка)

Прошито, пронумеровано на

(девят) листах

Председатель Правления КПК «Имист»

/Мишустин Р.Г./
(ФИО)

(подпись)

