ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

«МОЗЫРСКИЙ ДЕРЕВООБРАБАТЫВАЮЩИЙ КОМБИНАТ»
(ОАО «МОЗЫРСКИЙ ДОК»)

УТВЕРЖДЕНО
приказом ОАО «Мозырский ДОК»
от «____» _____2023г. №_____

ПОЛОЖЕНИЕ О СИСТЕМЕ УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

г. Мозырь 2023

Предисловие

1. ДОКУМЕНТ РАЗРАБОТАН начальником Службы безопасности и защиты информации, начальником сектора информационных технологий Открытого акционерного общества «Мозырский деревообрабатывающий комбинат» (далее – Общество).
2. УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Общества №___ от «___» _____2023 года.
3. ДАТА ВВЕДЕНИЯ «____» _____ 2023 года.
4. ВВЕДЕН ВПЕРВЫЕ.
5. СРОК ДЕЙСТВИЯ - до замены (отмены).
6. Оригинал документа хранится: 1 экземпляр – в Службе безопасности и защиты информации Общества, 2 экземпляр – в секторе информационных технологий Обществ.
7. Аннотация.

Документ является основополагающим организационно-методическим документом в отношении обеспечения информационной безопасности, направленной на защиту информации при осуществлении деятельности в Открытом акционерном обществе «Мозырский деревообрабатывающий комбинат».

8. Лица, ответственные за документ, - начальник службы безопасности и защиты информации, начальник сектора информационных технологий Открытого акционерного общества «Мозырский деревообрабатывающий комбинат».

СОДЕРЖАНИЕ

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Положение о системе управления и обеспечения информационной безопасностью в Обществе (далее - Положение) определяет общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, в том числе и персональных данных, документально закрепленные собственником информационной системы Общества.

2. Положение разработано с учетом требований Закона Республики Беларусь от 10.11.2008 № 455-З (ред. от 11.05.2016) «Об информации, информатизации и защите информации», Положения об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации, утвержденным Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» (Национальный реестр правовых актов Республики Беларусь, 2011 г., № 121, 1/13026), Положением о технической и криптографической защите информации в Республике Беларусь, утвержденным Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» (Национальный правовой Интернет-портал Республики Беларусь, 18.04.2013, 1/14225), техническими нормативными правовыми актами, Положением о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 11.10.2017 № 64).

3. Положение служит основой для разработки локальных правовых актов, регламентирующих в Обществе вопросы защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено.

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

5. В настоящей Положении под термином «сотрудник» понимаются все работники Общества. На лиц, работающих в Общества по договорам гражданско-правового характера, в том числе прикомандированных, положения настоящего Положения распространяются в случае, если это обусловлено в таком договоре.

ГЛАВА 2
ЦЕЛИ И ПРИЧИНЫ ЗАЩИТЫ ИНФОРМАЦИИ

6. Целями и причинами защиты информации являются:

6.1. сохранение конфиденциальности информационных ресурсов;

6.2. обеспечение непрерывности доступа к информационным ресурсам Общества для поддержки бизнес-деятельности;

6.3. защита целостности деловой информации с целью поддержания возможности Общества по оказанию услуг высокого качества и принятию эффективных управленческих решений.

6.4. своевременное выявление и оценка причин, условий и характера угроз информационной безопасности, а также дальнейшее прогнозирование развития событий на основе мониторинга инцидентов информационной безопасности.

ГЛАВА 3
НАЗНАЧЕНИЕ НАСТОЯЩЕГО ПОЛОЖЕНИЯ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

7. Повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Общества. Обеспечение правового режима использования документированной информации как объекта интеллектуальной собственности и защиты в Обществе. Обеспечение правомочности обращений пользователей и вычислительных процессов к системным, информационным сетевым ресурсам информационных систем в Обществе.

8. Определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Общества.

9. Обеспечение регулярного контроля за соблюдением положения и проведение периодических проверок соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору Общества.

ГЛАВА 4
ОБЛАСТЬ ПРИМЕНЕНИЯ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

10. Требования настоящего Положения распространяются на всю информацию и ресурсы обработки информации Общества. Соблюдение настоящего Положения обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации Общества, должна быть оговорена обязанность третьего лица по соблюдению требований настоящего Положения.

11. Обществу принадлежат на праве собственности (в том числе на праве интеллектуальной 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 Общества, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и сотрудников Общества.

ГЛАВА 5
ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ И СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

12. В Обществе используется информационная система, в которой обрабатываются персональные данные, за исключением специальных персональных данных, и которая не имеет подключений к открытым каналам передачи данных, отнесенная к соответствующему классу 4-ин типовых информационных систем.

13. Закупка персональных компьютеров, сетевого оборудования и иных аппаратно-программных комплексов проводится по согласованию с сектором информационных технологий.

ГЛАВА 6
СВЕДЕНИЯ О ПОДРАЗДЕЛЕНИИ ЗАЩИТЫ ИНФОРМАЦИИ

14. В Обществе подразделением защиты информации, ответственным за обеспечение защиты информации, в том числе и персональных данных, является Служба безопасности и защиты информации, по вопросам технического обеспечения и защиты – сектор информационных технологий.

15. Основными задачами Службы безопасности и защиты информации и сектора информационных технологий являются:

15.1. разработка и внедрение организационных и технических мероприятий по комплексной защите информации Общества;

15.2. сохранение конфиденциальности документированной информации;

15.3. разработка текущих и перспективных планов работ по комплексной защите информации Общества;

15.4. внедрение технических средств контроля по комплексной защите информации Общества;

15.5. обеспечение контроля за соблюдением нормативных требований по надежной защите информации;

15.7. обеспечение комплексного использования технических средств и организационных мероприятий для защиты информации Общества.

15.8. проведение служебных расследований по выявленным фактам нарушений информационной безопасности, а также принятие мер по устранению причин, условий и возможных негативных последствий нарушений.

ГЛАВА 7

ПРЕДОСТАВЛЕНИЕ ПРАВ ДОСТУПА И КОНТРОЛЬ ИНФОРМАЦИОННЫХ СИСТЕМ

16. Все работы в пределах территории Общества выполняются в соответствии с должностными обязанностями или рабочими инструкциями только на компьютерах, разрешенных к использованию в Обществе.

17. Внос в здания и помещения Общества личных портативных компьютеров и внешних носителей информации (диски, флэш-карты и т. п.), а также вынос их за пределы Общества производится только при согласовании с начальником Службы безопасности и защиты информации на основании служебной записки (приложение).

18. Все данные, составляющие коммерческую тайну Общества, должны хранится исключительно на жестких дисках персональных компьютеров Общества. Все персональные компьютеры Общества должны быть внесены в корпоративный домен MOZ-DOK.

19. Непосредственный допуск к информационным ресурсам Общества (электронная почта, система электронного документооборота и т.д.) осуществляется на основании заявок, подписанных должностными лицами, ответственными за эти ресурсы, и по согласованию со службой безопасности и защиты информации, ответственными за организацию работы (сектор информационных технологий) (приложение).

Перед допуском работника к информационной системе его непосредственный руководитель обязан организовать изучение работником документов, устанавливающих требования информационной безопасности в Обществе и защиты информации в информационных системах, а также провести обучение навыкам выполнения процедур, необходимых для использования информационных ресурсов, правилам работы с конфиденциальной информацией и документами её содержащими. По завершению обучения в письменной форме предоставить на него заявку по допуску к информационным ресурсам.

Каждый работник, допускаемый к информационным системам Общества, должен быть проинформирован об ответственности за нарушения режима информационной безопасности.

В целях обеспечения доступа к информационному ресурсу любой вход в систему должен осуществляться пользователем с использованием идентификатора (личной учётной записи) в соответствии, с которым пользователь работает в информационных системах.

19.1. работа нескольких пользователей под одним идентификатором (учетной записью) не допускается;

19.2. создание обезличенных идентификаторов (учетных записей) не допускается;

19.3. в целях администрирования (осуществления настроек) сетевых сервисов допускается создание технических учетных записей, права доступа которых ограничены полномочиями, необходимые для работы конкретного сетевого ресурса;

19.4. технические учетные записи должны быть закреплены за конкретными работниками, осуществляющими поддержку конкретного сетевого ресурса;

19.5. регистрация пользователя, предоставление ему прав доступа к информационным ресурсам, их изменение и блокировка производится сектором информационных технологий на основании служебной записки (заявки) согласованной с начальником Службы безопасности и защиты информации (приложение).

20. Порядок выбора и использование паролей.

Пароли подразделяются на группы:

-первоначальный (временный, одноразовый) пароль;

-пользовательские пароли.

При выборе паролей (в том числе и первоначального пароля), используемых в процессе аутентификации вход в информационную систему Общества, следует использовать пароли, отвечающие следующим требованиям сложности:

-длина пользовательского пароля должна быть, не менее 8 символов.

-среди символов пароля обязательно должны присутствовать несколько наборов символов, буквы в верхнем и нижнем регистрах, цифры и специальные символы (#$%^);

-нельзя использовать словарные слова (имена, фамилии, название организации, торговые марки и.т.д.) слова записанные транслитерацией (пароль-parol) русские слова, набранные на латинской раскладке (пароль-gfhjkm);

-для повышения степени защищенности информационной системы Общества применено ограничение на количество неудачных попыток при вводе пользовательских паролей, после 3х неудачных попыток входа, учётная запись пользователя блокируется.

-пароль генерируется на этапе создания учётной записи пользователя специалистом сектора информационных технологий. Генерация пароля происходит случайным образом.

Передача паролей по телефону категорически запрещается. Передача паролей по другим каналам связи (мессенджеры (Viber, Telegram и т.д.)) а также электронной почте категорически запрещается.

Восстановление забытого пользовательского пароля осуществляется после доклада руководителю структурного подразделения, после чего руководителем структурного подразделения составляется заявка на восстановление забытого пароля, или генерацию нового пароля, согласовывается с начальником службы безопасности и защиты информации и начальником сектора информационных технологий.

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

ГЛАВА 8
ДОСТУП ТРЕТЬИХ ЛИЦ К ИНФОРМАЦИОННЫМ СИСТЕМАМ ОБЩЕСТВА

22. Доступ работников Общества и сторонних организаций к работам по разработке, внедрению и эксплуатации информационных систем осуществляется в соответствии с действующими требованиями, установленными Положением о коммерческой тайне в Обществе и регламентами по использованию информационных ресурсов Общества.

Решение о предоставлении доступа третьим лицам к информационным активам инициируется работником Общества ответственным за взаимодействие с третьим лицом.

Каждый сотрудник обязан немедленно уведомить Службу безопасности и защиты информации, сектор информационных технологий обо всех случаях обращений предоставления доступа третьим лицам к информационным активам.

23. Доступ третьих лиц к информационным активам Общества осуществляется на основании заявки на доступ, согласованной со Службой безопасности и защиты информации и сектором информационных технологий (приложение).

ГЛАВА 9
УДАЛЕННЫЙ ДОСТУП

24. Пользователи получают право удаленного доступа к информационным ресурсам Общества с учетом их взаимоотношений с Организацией. Удаленный доступ пользователям предоставляется на основании докладной записки согласованной с начальником Службы безопасности и защиты информации и начальником Сектора информационных технологий.

25. Сотрудникам, использующим в работе портативные компьютеры Общества, может быть предоставлен удаленный доступ к сетевым ресурсам Общества исключительно по средствам VPN.

26. Сотрудникам, работающим за пределами Общества с использованием компьютера, не принадлежащего Общества, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ. Удалённый доступ предоставляется по средствам установки и подключение пользователя через VPN. Доступ к рабочим фалам допускается исключительно через удалённый рабочий стол (пользователь подключится к своему рабочему компьютеру). В исключительных случаях, когда необходимо оперативное подключение, допускается использовать системы удалённого доступа такие как AnyDesk или TeamViewer.

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

28. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Общества, должны иметь программное обеспечение антивирусной защиты с последними обновлениями.

ГЛАВА 10
ДОСТУП К СЕТИ ИНТЕРНЕТ

29. В случае если пользователю требуется доступ в Интернет, заявка на предоставление доступа, визируется заместителем директора курирующее данное структурное подразделение и согласовывается с начальником Службы безопасности и защиты информации и начальником сектора информационных технологий (приложение). Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

30. Рекомендованные правила:

30.1. сотрудникам Общества разрешается использовать сеть Интернет только в служебных целях;

30.2. 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;

30.3. сотрудники Общества перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

30.5. запрещен доступ в интернет через сеть Общества для всех лиц, не являющихся сотрудниками Общества, включая членов семьи сотрудников Общества.

31. служба безопасности и защиты информации, сектор информационных технологий имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

ГЛАВА 11

ЗАЩИТА ОБОРУДОВАНИЯ И ПОРЯДОК ХРАНЕНИЯ ПАРОЛЕЙ

32. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация Общества.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят специалисты сектора информационных технологий. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

33. Пользователь обязан помнить свой пароль.

33.1. записывать пароль на листках, календарях, корпусах оборудования, в записных книжках и и.т.п. запрещается;

33.2. пользователю категорический запрещено сообщать свой пароль кому бы то ни было;

33.3. запрещено узнавать, подбирать, использовать чужие пароли доступа к информационной системе Общества;

33.4. пользователь обязан хранить копии паролей в конверте. Конверт должен быть запечатан и хранится у руководителя структурного подразделения в недоступном месте;

33.5. конверт может быть вскрыт руководителем в порядке исключения;

33.6. смена паролей пользователя производится в случай:

-при компрометации пользовательского пароля к соответствующему элементу информационной системы Общества. Пароль считается скомпрометированным, если пользователям или работникам, проводящим расследование инцидентов, известно или есть основания полагать, что пароль стал известен третьим лицам.

-при изменении служебных полномочий (переход в другое подразделение);

-при увольнении, либо изменении служебных полномочий специалиста сектора информационных технологий;

-в случае, если пароль забыт.

33.7. в ситуации, когда возникла необходимость вести пароль пользователя в его отсутствие с целью предотвращения прерывания критических бизнес-процессов, руководитель структурного подразделения вскрывает конверт с копией пароля, с обязательным уведомлением пользователя о факте и цели вскрытия. Пользователь, чей пароль был вскрыт, после этого обязан сменить пароль при первой возможности.

В случае, если пользователь забыл пароль, пароль не считается скомпрометированным.

ГЛАВА 12
АППАРАТНОЕ ОБЕСПЕЧЕНИЕ

34. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа «компьютерная мышь»), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и коммутаторы) для целей настоящей Политики вместе именуются компьютерным оборудованием.

Компьютерное оборудование, предоставленное Организацией, является ее собственностью и предназначено для использования исключительно в производственных целях.

35. Пользователи персональных компьютеров, содержащих информацию, составляющую коммерческую тайну Общества, 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.

36. Каждый сотрудник, получивший в пользование персональный компьютер, обязан принять надлежащие меры по обеспечению его сохранности. В ситуациях, когда возрастает степень риска кражи персонального компьютера, например, в гостиницах, аэропортах, в офисах деловых партнеров и т. д., пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра.

37. Во время поездки в автомобиле персональный компьютер должен находиться в салоне автомобиля. На ночь его следует перенести из автомобиля в помещение.

38. 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.

39. 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. После отформатировать носитель.

40. Мобильные телефоны, имеющие функцию электронной почты, и прочие переносные устройства не относятся к числу устройств, имеющих надежные механизмы защиты данных. В подобных устройствах не рекомендуется хранить конфиденциальную информацию.

41. USB порты передачи данных, в персональных компьютерах сотрудников Общества блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись информации у службы безопасности и защиты информации, специалиста отдела сектора информационных технологий.

ГЛАВА 13
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

42. Все программное обеспечение, установленное на предоставленном Обществом компьютерном оборудовании, является собственностью Общества и должно использоваться исключительно в производственных целях.

43. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании программное обеспечение, не входящее в список разрешенных (приложение), нелицензионное 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 непосредственному руководителю сотрудника и в Службу безопасности и защиты информации для проведения проверки.

44. На всех персональных компьютерах программное обеспечение устанавливается при настройке компьютера, исключительно специалистом сектора информационных технологий и исключительно из перечисленного списка допустимых для установки программных средств (приложение). Если появляется необходимость установки программного обеспечения, которое не входит в список допустимых для установки программных средств, необходимо написать заявку с обоснованием необходимости установку данного ПО руководителю Общества и согласовать ее с начальником службы безопасности и защиты информации, начальником сектора информационных технологий и.

45. Все компьютеры, подключенные к сети Общества, должны быть оснащены системой антивирусной защиты.

46. Сотрудники Общества не должны:

46.1. блокировать антивирусное программное обеспечение;

46.3. изменять настройки и конфигурацию установленного программного обеспечения.

46.4. устанавливать на компьютеры мессенджеры (Viber, Telegram и.т.д.)

47. Организация предпочитает приобретать программное обеспечение, а не разрабатывать собственные программы, поэтому пользователям, желающим внедрить новые программные комплексы, необходимо согласовать свое предложение со специалистами сектора информационных технологий, начальником службы безопасности.

ГЛАВА 14
РЕКОМЕНДУЕМЫЕ ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

48. 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 стандартам Общества в области деловой этики.

49. Запрещается использовать почтовые ящики для служебной переписки на mail.yandex, mail.ru, rambler.ru, mail.google и иные.

50. Сотрудникам запрещается направлять партнерам конфиденциальную информацию Общества по электронной почте без использования систем шифрования.

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

Отправка сообщений, содержащих коммерческую тайну и иные конфиденциальные сведения по открытым (не защищенным) каналам передачи данных, в том числе через Интернет, запрещается.

51. Сотрудникам Общества запрещается использовать личные почтовые ящики электронной почты для осуществления деятельности Общества.

52. Запрещается использование сотрудниками Общества личных почтовых ящиков электронной почты и облачных ресурсов хранение информации на рабочих персональных компьютерах.

53. Сотрудники Общества для обмена документами с бизнес-партнерами должны использовать только свой официальный адрес электронной почты.

54. Сообщения, пересылаемые по электронной почте, имеют тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

55. 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

Службу безопасности и защиты информации и специалистов отдела информационных технологий.

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

57. Недопустимые действия и случаи использования электронной почты:

57.1. рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

57.2. рассылка рекламных материалов, не связанных с деятельностью Общества;

57.6. 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 стандартам Общества в области этики.

58. При приеме сообщений запрещается:

- Открывать сообщения, для которых имеется предупреждение о возможном наличии вируса.

- Открывать сообщения, у которых поле «От:» («From:») указаны адреса подозрительного характера (например: shopping4.gmobb.jp и прочие отличающиеся от привычных доменов @mail.ru, @yandex.ru, @gmail.com или не принадлежащие домену организации) с просьбой перейти по ссылке, заполнить данные. При получении такого письма, необходимо уведомить специалистов сектора информационных технологий путем перенаправки письма специалисту для последующего анализа.

59. 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 Общества процедурами документооборота.

60. Пересылка значительных объемов данных в одном сообщении может отрицательно повлиять на общий уровень доступности сетевой инфраструктуры Общества для других пользователей. Объем вложений не должен превышать 15 Мбайт.

ГЛАВА 15
СООБЩЕНИЯ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕАГИРОВАНИЕ И ОТЧЕТНОСТЬ

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

авторизированного пользователя блокируются (либо ограничиваются) до завершения рассмотрения инцидента.

62. В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте начальнику службы безопасности и защиты информации, начальнику сектора информационных технологий.

63. Пользователи должны проинформировать об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

64. Если имеется подозрение или выявлено наличие компьютере пользователя деструктивной составляющей (выявлен вирус, заблокирован доступ и ресурсу):

64.1. проинформировать службу безопасности и зашиты информации, специалистов сектора информационных технологий;

64.2. не использовать персональный компьютер в работе до решения проблемы;

64.3. не подсоединять этот компьютер к компьютерной сети Общества до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование специалистами сектора информационных технологий.

ГЛАВА 16
ПОМЕЩЕНИЯ С ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

65. Конфиденциальные встречи (заседания) должны проходить только в защищенных техническими средствами информационной безопасности помещениях.

66. Перечень помещений с техническими средствами информационной безопасности утверждается директором Общества.

67. Участникам заседаний запрещается входить в помещения с записывающей аудио/видеоаппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами без предварительного согласования с службой безопасности и защиты информации.

68. Доступ участников конфиденциального заседания в помещение для его проведения осуществляется на основании утвержденного перечня, контроль за которым ведет лицо, отвечающее за организацию встречи.

ГЛАВА 17
УПРАВЛЕНИЕ СЕТЬЮ

69. Уполномоченные специалисты сектора информационных технологий контролируют содержание всех потоков данных, проходящих через сеть Общества.

70. Сотрудникам Общества запрещается:

70.1. нарушать информационную безопасность и работу сети Общества;

70.2. сканировать систему на наличие уязвимостей;

70.3. перехватывать данные других сотрудников;

70.4. получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя;

70.5. использовать любые программы, команды с целью вмешаться в работу или нарушать работу пользователя и его устройства;

70.6. передавать информацию о сотрудниках или списки сотрудников Общества посторонним лицам;

70.7. распространять компьютерные вирусы и прочее вредоносное программное обеспечение.

ГЛАВА 18
ЗАЩИТА И СОХРАННОСТЬ ДАННЫХ

71. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях. Специалисты сектора информационных технологий обязаны оказывать пользователям содействие в проведении резервного копирования данных на соответствующие носители.

72. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

73. Только специалисты сектора информационных технологий на основании заявок руководителей подразделений, согласованных со Службой безопасности и защиты информации могут создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

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

75. Все заявки на проведение технического обслуживания компьютеров должны направляться в сектор информационных технологий с последующим информированием службы безопасности и защиты информации.

ГЛАВА 19
РАБОТА СО СМЕНЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ

76. Использование сменных носителей информации в информационной системе Общества без разрешения запрещено.

77. Право использования сменных носителей информации предоставляется после согласования заявки на предоставление доступа к внешним устройствам (приложение) непосредственным руководителем Пользователя, а также с начальником Службы безопасности и защиты информации и начальником сектора информационных технологий.

78. Обмен рабочими документами должен производиться через систему электронного документооборота «1С Документооборот» или через корпоративную электронную почту.

ГЛАВА 20
РАБОТА С КРИПТОГРАФИЧЕСКИМИ СИСТЕМАМИ

76. К работе с криптографическими системами допускаются только сотрудники Общества, имеющие соответствующее разрешение от директора Общества.

77. Криптографические ключи электронно-цифровых подписей должны храниться в сейфах или запирающихся ящиках под ответственностью уполномоченных лиц. Доступ неуполномоченных лиц к носителям секретных ключей и шифрования должен быть исключен.

78. Категорически запрещается:

78.1. предоставлять доступ к криптографическим ключам электронно-цифровых подписей другим лицам;

78.2. устанавливать программное обеспечения для доступа и управления криптографическим ключам электронно-цифровых подписей на персональный компьютер пользователя, которому не принадлежит этот ключ;

79. При компрометации криптографического ключа электронно-цифровых подписей и прочей электронной информации Общества принимаются меры для прекращения любых операций с использованием этих ключей и прочей информации; принимаются меры для смены ключей и паролей. По факту компрометации организуется служебное расследование, результаты которого отражаются в акте и доводятся до сведения директора Общества.

ГЛАВА 21
РАЗРАБОТКА СИСТЕМ И УПРАВЛЕНИЕ ВНЕСЕНИЕМ ИЗМЕНЕНИЙ

80. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы и согласованы с начальником Службы безопасности и защиты информации и начальником сектора информационных технологий.

81. Подразделениями службы безопасности и информационных технологий Обществ, организуется и осуществляется контроль за порядком обращения с конфиденциальной информацией и информационными ресурсами работниками производственных и обеспечивающих подразделений Общества.

Начальник Службы безопасности
и защиты информации В.К. Косинский

Приложение 1 Форма заявки на доступ к информационным активам

Директору ОАО «Мозырский ДОК»
А.В. Иванову

Заявка на доступ к информационным активам

В связи служебной необходимость (для чего именно мониторинг цен и.т.д.) прошу Вас обеспечить (если требуется установка нового ПК) и подключить к нижеперечисленным информационным активам следующих работников:

1._____
(должность, ФИО полностью) на срок (бессрочно/до <дата>)

2. _____
(должность, ФИО полностью) на срок (бессрочно/до <дата>)

Наименование информационного актива	**Функциональные задачи в подсистеме и тип доступа**	**Должность, ФИО ответственного за допуск**	**Подпись**
Электронная почта		Начальник структурного подразделения	
1С Документооборот		Начальник структурного подразделения	
1С Бухгалтерия		Начальник структурного подразделения	
1С ERP		Начальник структурного подразделения	
1С Зарплата и управление персоналом		Начальник структурного подразделения	
Электронная почта		Начальник структурного подразделения	
Иной сетевой ресурс		Начальник структурного подразделения	

По своим служебным обязанностям будет работать со следующими сведениями, составляющими коммерческую тайну (согласно Перечню):

_____ _____ _____
руководитель структурного подразделения подпись Ф.И.О.

«___» _____ 20__ г.

Согласовано:
Начальник службы безопасности и защиты информации

_____ _____
подпись (И.О. Фамилия)
«___» _____ 202__ г.

Согласовано:
Начальник сектора информационных технологий

_____ _____
подпись (И.О. Фамилия)
«___» _____ 202__ г.

Приложение 2 Форма заявки на удаленный доступ к корпоративной сети

Директору ОАО «Мозырский ДОК»
А.В. Иванову

Заявка на удаленный доступ к корпоративной сети

В связи служебной необходимость прошу Вас предоставить доступ к корпоративной сети включить в группу удаленного доступа к Web-приложениям, удаленного доступа к сетевым ресурсам следующих работников:

1._____
(должность, ФИО полностью) на срок (бессрочно/до <дата>)

2. _____
(должность, ФИО полностью) на срок (бессрочно/до <дата>)

По своим служебным обязанностям будет работать со следующими сведениями, составляющими коммерческую тайну (согласно Перечню)

_____ _____

руководитель структурного подразделения подпись Ф.И.О.

«___» _____ 20__ г.

Согласовано:
Начальник службы безопасности и защиты информации

_____ _____
подпись (И.О. Фамилия)
«___» _____ 202__ г.

Согласовано:
Начальник сектора информационных технологий

_____ _____
подпись (И.О. Фамилия)

«___» _____ 202__ г.

Приложение 3 Форма заявки на блокировку доступа к информационным активам

Директору ОАО «Мозырский ДОК»
А.В. Иванову

Заявка на блокировку доступа к информационным активам

В связи служебной необходимость прошу Вас отозвать все права доступа к информационным активам следующих работников:

1._____
(должность, ФИО полностью)

2. _____
(должность, ФИО полностью)

_____ _____
руководитель структурного подразделения подпись
Ф.И.О.
«___» _____ 20__ г.

Согласовано:
Начальник службы безопасности и защиты информации

_____ _____
подпись (И.О. Фамилия)
«___» _____ 202__ г.

Согласовано:
Начальник сектора информационных технологий

_____ _____
подпись (И.О. Фамилия)

«___» _____ 202__ г.

Приложение 4 Форма заявки на предоставление доступа к внешним устройствам

Директору ОАО «Мозырский ДОК»
А.В. Иванову

Заявка предоставление доступа к внешним устройствам

В связи служебной необходимость предоставления информации в налоговую инспекцию (согласно письма №123 от12.09.2022) прошу Вас предоставить доступ работнику Сидорову В.А.

№ п\п	Наименование/модель устройства	Серийный (регистрационный) номер	Срок использования

_____ _____ _____
руководитель структурного подразделения подпись Ф.И.О.

«___» _____ 20__ г.

Согласовано:
Начальник службы безопасности и защиты информации

_____ _____
подпись (И.О. Фамилия)
«___» _____ 202__ г.

Согласовано:
Начальник сектора информационных технологий

_____ _____
подпись (И.О. Фамилия)

«___» _____ 202__ г.

Приложение 5

ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

5.1 Субъекты информационных отношений в пределах предоставленных им полномочий и (или) прав при использовании объектов информационных отношений имеют право:

использовать ОИС для доступа к ИС и ИР, другим ОИС с целями поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления и пользования информацией;

осуществлять иные действия в соответствии с должностными инструкциями и ЛПА Общества.

5.2 Субъекты информационных отношений в пределах предоставленных им полномочий и (или) прав при использовании объектов информационных отношений обязаны:

соблюдать права других лиц при использовании объектов Общества;

исполнять обязанности в соответствии с должностными инструкциями и ЛПА актами Общества.

5.3 Права и обязанности субъектов Общества регламентированы следующими документами:

политикой информационной безопасности;

положением о системе управления и обеспечения информационной безопасностью;

должностными инструкциями работников Общества;

5.4 Общество обязуется постоянно совершенствовать систему информационной безопасности, обеспечивать ресурсами, достаточными для достижения указанных в настоящей политике целей, а также соответствовать всем обязательным и\или применимым законодательным, нормативным, договорным и иным требованиям.

Приложение 6

Памятка по информационной безопасности

Всем пользователям корпоративной системы должны быть известны простые правила безопасности:

использовать и периодически менять сложные пароли, никогда не передавать средства идентификации – пароль и логин – другим сотрудникам;

не хранить в «облаках» конфиденциальную информацию, даже если нужно поработать с годовым отчетом из дома;

уничтожать ненужные документы в шредере;

не передавать информацию без официального запроса;

не смешивать корпоративную и личную почту;

архивировать важные файлы;

блокировать компьютер перед уходом с рабочего места;

уметь распознавать фишинговые письма;

ознакомиться с практиками социальной инженерии и не поддаваться им.

Приложение 7

Памятка удалённый доступ

Правила, позволяющие сделать такие удаленные рабочие отношения максимально безопасными:

исключить возможность использования удаленными сотрудниками для подсоединения к корпоративной сети открытых Wi-Fi-сетей, в которых возможен перехват трафика;

домашние сети сотрудников должны быть защищены паролями и шифрованием как минимум уровня WPA2. В компании необходимо разработать правила информационной безопасности для удаленных сотрудников для защиты домашних сетей;

подключение для мобильных устройств к корпоративной сети должно происходить только по каналам VPN. Компании желательно самой выбрать надежного поставщика услуг VPN и обеспечить сотрудникам на удаленном доступе возможность работать с этим сервисом;

для работы необходимо иметь отдельное мобильное устройство и не смешивать частную и корпоративную информацию, система ИБ компании должна предусматривать меры защиты таких удаленных устройств;

сведения о работе на удаленном доступе не должны публиковаться в социальных сетях, чтобы не вызвать интерес злоумышленников. Устное и письменное разглашение конфиденциальных данных недопустимо;

пароли на ресурсах, связанных с работой на удаленном доступе, необходимо регулярно менять;

плагины и программное обеспечение, содержащие известные хакерам уязвимости (например, Adobe Flash, Acrobat Reader, Java и другие), должны регулярно обновляться;

компьютер и мобильные устройства нужно защищать паролем даже дома, чтобы гость или ремонтный рабочий не смогли похитить или случайно повредить данные.

Приложение 8 (список допустимых для установки на компьютеры пользователей программного обеспечения)

Офисное программное обеспечение:

Для работы с офисными документами Word, Excel, создание презентаций: Microsoft Office

Для работы с документами PDF: PDF-XChange Viewer, Adobe Acrobat Reader, ABBYY FineReader

Для работы с текстовыми файлами: Notepad++

Для работы с архивами: 7-Zip, WinRar

Для работы со сканером: WinScan2PDF (или иной который необходимый для работы со сканером, если не подходит WinScan2PDF)

Просмотр картинок или фотографий: IrfanView

Просмотр медиафайлов: VLC Player

Программное обеспечение для работы в сети интернет:

Веб браузеры: Google Chrome, Mozilla Firefox

Работа с электронной почтой: Microsoft Outlook, или работа непосредственно из браузера

Системное программное обеспечение:

Управление файлами: Total Commander

Антивирус: Symantec Endpoint Protection

Программы для удалённого управления: AnyDesk, MeshCentral