Открытое акционерное общество
«Ратон»

УТВЕРЖДАЮ
Директор
_____М.Г.Приходько
«21» 06 2024

ПОЛОЖЕНИЕ
«О Политике информационной
безопасности ОАО «Ратон»
П- 43 -2024
г.Гомель

Глава 1
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В Политике информационной безопасности ОАО «Ратон» (далее – Политика) используются следующие термины и определения:

автоматизированная обработка ПД – обработка ПД с помощью средств вычислительной техники;

анонимайзер – средство для скрытия информации о компьютере, его IP-адресе или пользователе в ЛВСП и Интернет;

антивирусное программное средство (АПС) – программное средство для предотвращения заражения вредоносным кодом файловых ресурсов компьютера, обнаружения компьютерных вирусов, лечения или удаления инфицированных файлов;

блокировка учетной записи пользователя – отключение учетной записи пользователя в ИС предприятия;

вирусное программное средство (далее – вирус) – программное средство, созданное злоумышленником, несанкционированно установленное и/или функционирующее на компьютере, приводящее к частичному или полному повреждению СЭД, ПС и прочих ресурсов ИС;

вирусное заражение ИС – неконтролируемое распространение вируса в ИС, приводящее к нарушению штатного режима её функционирования;

дистанционная работа– исполнение работником своих трудовых обязанностей с использованием удаленного доступа;

информационная система предприятия (ИС) – совокупность технического программного и организационного обеспечения, сетевых ресурсов предприятия, предназначенная для своевременного обеспечения надлежащих работников надлежащей информацией;

информационный ресурс – организованная совокупность документированной информации, включающая базы данных и знаний, другие массивы информации в ИС;

информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления;

информационная безопасность (ИБ) – сохранение целостности, конфиденциальности и доступности информационных ресурсов предприятия;

инцидент ИБ –непредвиденное или нежелательное событие, которое может нарушить целостность, доступность или конфиденциальность информационных ресурсов предприятия и создает угрозу ИБ;

исполняемые файлы – файлы, содержащие в себе готовые к запуску компьютерные программы (включают приложения, динамические библиотеки, драйвера, скрипты, пакетные файлы);

компьютер – электронное устройство, предназначенное для передачи, хранения и обработки информации;

компьютер для УД (удаленный доступ) – компьютер, принадлежащий предприятию, используемый Работником для осуществления удаленного доступа;

компрометация – факт несанкционированного доступа к защищаемой информации, а также подозрение осуществления такого доступа;

личный компьютер – компьютер, не принадлежащий предприятию, используемый Работником для осуществления удаленного доступа;

логин – имя учетной записи пользователя в ИС;

локальная вычислительная сеть предприятия (ЛВСП) –система передачи информации между двумя или более компьютерами и/или компьютерным оборудованием, находящаяся на географически ограниченной территории пользователя;

менеджмент инцидентов ИБ – деятельность по своевременному обнаружению инцидентов ИБ, оперативному реагированию на них в интересах минимизации и/или ликвидации негативных последствий для предприятия при нарушениях ИБ;

мессенджер – программа для мгновенного обмена в Интернет текстовыми сообщениями, аудиозаписями, фотографиями и другими мультимедиа-файлами;

носитель электронных данных (НЭД) – материальный объект, используемый для хранения или передачи информации;

несанкционированный доступ – доступ пользователя к ресурсам ИС в нарушение своих должностных полномочий или доступ к ресурсам ИС лица, не имеющего соответствующего разрешения на доступ к ним;

обработка ПД (персональные данные) – любое действие (операция) или совокупность действий (операций) с ПД, совершаемых с использованием средств автоматизации или без их использования;

пароль – набор знаков, предназначенный для подтверждения личности работника предприятия как пользователя, используемый для защиты служебных электронных данных ИС от несанкционированного доступа;

персональные данные (ПД) –информация, определяемая документом «Порядок доступа к персональным данным, обрабатываемым в информационной системе ОАО «Ратон»;

пользователь – работник предприятия, использующий ресурсы ИС для выполнения своих должностных обязанностей, для которого в ИС имеется

(заведена) соответствующая учетная запись с её идентификатором, сведениями и описаниями (в т.ч. логин и пароль);

постороннее лицо – лицо, не имеющее разрешения на доступ к ресурсам ИС;

предприятие – ОАО «Ратон».

предоставление ПД – действия, направленные на раскрытие (распространение) ПД третьим лицам;

программное средство (ПС) –алгоритм, реализованный в виде последовательности действий для исполнения компьютером;

работник предприятия (работник) – лицо, работающее по трудовому договору (контракту);

рабочее время – время работы в соответствии с режимом работы Работника, закрепленным локальными нормативными правовыми актами;

рабочий день – период рабочего времени, установленный производственным календарем;

рабочий компьютер – компьютер, находящийся на рабочем месте работника на предприятии;

сброс пароля пользователя – процесс взаимодействия пользователя (включая подачу заявки пользователем) и системного администратора предприятия по установке первоначального пароля для пользователя, зарегистрированного в ИС;

системный диск – логический диск компьютера, на который установлена операционная система;

СИБ – система информационной безопасности;

служебные электронные данные (СЭД) – компьютерные файлы и информационные ресурсы, необходимые работникам предприятия для выполнения должностных обязанностей;

событие ИБ – идентифицированное возникновение состояния ИС, указывающее на возможное нарушение политики ИБ, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью;

субъект ПД – физическое лицо, в отношении которого осуществляется обработка ПД;

машинный носитель информации (МНИ) –любое техническое устройство либо физическое поле, предназначенное для фиксации, хранения, накопления, преобразования и передачи компьютерной информации;

удаленный доступ (УД) – возможность осуществления работы (мероприятий, действий) в ИС с территориально удаленного от предприятия компьютера с использованием информационно-коммуникационных технологий;

учетная запись пользователя – запись в базах данных ИС, хранящая сведения о пользователе;

угроза ИБ – вероятность нарушения целостности, доступности или конфиденциальности информационных ресурсов предприятия;

электронная почта предприятия (ЭП) – технология и предоставляемые ею услуги по пересылке и получению информации в форме электронных сообщений по распределённой (в том числе по ЛВСП, глобальной сети Интернет) компьютерной сети.

Глава 2.
ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика разработана в соответствии с законодательством Республики Беларусь в части обеспечения ИБ и определяет цели, задачи и принципы обеспечения ИБ на ОАО «Ратон».

2. Политика устанавливает общие намерения и направления деятельности по обеспечению конфиденциальности, целостности, сохранности, подлинности и доступности информации на предприятии.

3. Целью Политики является обеспечение ИБ предприятия от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ИС.

4. Основными задачами деятельности по обеспечению ИБ ИС являются:

своевременное выявление и оценка источников угроз ИБ, причин и условий их возникновения;

предотвращение инцидентов;

разграничение доступа пользователей к информационным ресурсам предприятия с целью обеспечения доступа только к тем ресурсам и операциям с ними, которые необходимы для выполнения возложенных на пользователей должностных обязанностей;

защита от несанкционированных изменений настроек и параметров ИС, а также защита ИС от внедрения несанкционированных программ, включая компьютерные вирусы;

защита информации от утечки по техническим каналам при ее обработке, хранении и передаче;

совершенствование системы ИБ.

5. Стратегия предприятия в области обеспечения ИБ и защиты информации включает соблюдение законодательства Республики Беларусь в области защиты информации, безопасности информационных технологий и персональных данных.

6. Требования по обеспечению ИБ, изложенные в Политике, обязательны к исполнению всеми работниками предприятия, а также сторонними лицами, привлекаемыми к работе с информационными ресурсами предприятия на договорной основе.

7. В случае нарушения требований ИБ виновные лица привлекаются к ответственности, предусмотренной действующим законодательством.

ГЛАВА 3
ОБЪЕКТЫ, ПРОЦЕССЫ И СОСТАВ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8. Поставленные цели и решение задач деятельности по обеспечению ИБ достигаются:

разработкой локальных правовых актов, регламентирующих процессы защиты информации предприятия;

строгим учетом подлежащих защите информационных ресурсов ИС (информации, ПС, документов, каналов связи, серверов, автоматизированных рабочих мест);

определением прав и зон ответственности работников предприятия по вопросам защиты информации;

подготовкой должностных лиц (работников), ответственных за организацию и осуществление мероприятий по обеспечению ИБ;

постоянным поддержанием необходимого уровня защищенности ИС;

применением организационных мероприятий и технических (программно-аппаратных) средств защиты ресурсов системы;

контроль соблюдения пользователями информационных ресурсов предприятия требований по обеспечению ИБ;

своевременное и регулярное создание резервных копий файловой системы (back-up) с сохранением на отдельных серверах или в облачных хранилищах данных;

осуществление настройки сетевого оборудования при необходимости использования удаленного доступа исключительно выделенным кругом лиц с указанием конкретных IP или MAC-адресов рабочих станций;

обязательное изменение заводских настроек (логин и пароль) вновь приобретаемого и монтируемого сетевого оборудования.

9. Объектами ИБ являются:

информационные ресурсы с ограниченным доступом, содержащие информацию, распространение и (или) предоставление которой ограничено;

процессы обработки информации в ИС, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

информационная инфраструктура, включающая технические и программные средства обработки, анализа, передачи и отображения информации, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены элементы информационной среды.

10. Для обеспечения ИБ могут использоваться средства (аппаратно-программные средства, системы, комплексы):

мониторинга ИБ;

предотвращения утечек информации, распространение и (или) предоставление которой ограничено, из ИС;

предотвращения атак на уровне хоста;

обнаружения и предотвращения вторжений;

защиты от вредоносного кода;

фильтрации и контроля интернет-трафика;

криптографической защиты информации и электронно-цифровой подписи;

сканирования уязвимостей;

централизованного управления доступом;

иные аппаратные и программные комплексы.

11. Защите подлежат все информационные ресурсы предприятия независимо от формы их представления и местонахождения в ИС.

12. Вся информация, обрабатываемая и хранящаяся в ИС, является собственностью предприятия.

13. Работникам запрещается обрабатывать, хранить или передавать в ИС информацию личного характера.

14. Построение СИБ осуществляется на основе следующих принципов:

14.1. Принцип осознанного принятия рисков. Риски объективно невозможно полностью ликвидировать, они могут снижаться или приниматься;

14.2. Принцип разрешения (запрещено все, что не разрешено). Доступ к какому-либо объекту или информационному процессу предоставляется только при наличии соответствующего правила, отраженного в соответствующем локальном правовом акте предприятия, а также защитных и (или) контрольных мерах;

14.3. Принцип разграничения доступа. Каждому пользователю предоставляется доступ к информации и её носителям в соответствии с его полномочиями;

14.4. Принцип достаточной стойкости. Потенциальные злоумышленники должны встречать препятствия в виде достаточно сложных вычислительных задач, неадекватно больших временных затрат и (или) вычислительных мощностей, однако, стоимость защиты не может превышать стоимость защищаемых информационных ресурсов;

14.5. Принцип непрерывности защиты. Обеспечение ИБ– процесс, осуществляемый всеми должностными лицами и работниками предприятия, который должен постоянно функционировать на всех уровнях внутри предприятия и каждый работник должен в этом принимать участие. Деятельность по обеспечению ИБ является составной частью повседневной деятельности предприятия и ее эффективность также зависит и от участия руководства предприятия в обеспечении ИБ;

14.6. Принцип персональной ответственности. Персональная ответственность предполагает возложение ответственности за обеспечение ИБ и системы ее обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму;

14.7. Принцип минимизации полномочий. Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том

14.8. случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей;

14.9. Принцип непрерывности и независимости протоколирования действий с информационными ресурсами ИС. Действия пользователей по доступу к информации, ее изменению, добавлению, удалению и т.п., изменение прав доступа, иные администраторские действия, проводимые в том числе работниками безопасности, должны протоколироваться и сохраняться в заданный период времени без возможности их удаления.

14.10.Реализация процессов ИБ и их организация регламентируются отдельными локальными правовыми актами предприятия (регламенты, положения и другие документы по отдельным видам деятельности в сфере информационного обеспечения).

14.11.Подразделением, осуществляющим реализацию и контроль процессов ИБ, является отдел АСУ.

14.12. На предприятии используют следующие типы средств защиты ИБ:

организационные – комплекс мер и средств организационно-правового (нормативные документы, локальные правовые акты предприятия) и организационно-технического характера (меры по обслуживанию информационной инфраструктуры предприятия);

аппаратные (технические) – специальные оборудования и устройства, предотвращающее утечки, защищающее от проникновения в ИС;

программные – специальные ПС, предназначенные для защиты, контроля, хранения информации;

программно-аппаратные – специальное оборудование с установленным ПС для защиты данных.

ГЛАВА 4
УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

15. Построение СИБ и реализация процессов ИБ осуществляется с учетом вероятных угроз информационным ресурсам ИС.

16. Угрозами ИБ являются:

хищение (несанкционированное копирование) информации;

уничтожение информации;

модификация (несанкционированное изменение) информации;

нарушение доступности (несанкционированное блокирование) информации;

отрицание подлинности информации;

навязывание ложной информации.

17. Виды угроз ИБ:

природная– обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех;

техногенная – технократическая деятельность, источниками которой является: средства связи; некачественные технические средства обработки

информации; некачественные программные средства обработки информации; другие технические средства, применяемые на предприятии;

антропогенная– источником является субъект, имеющий доступ (санкционированный или несанкционированный) к работе со средствами защищаемого объекта.

18. Субъекты (источники), действия которых могут привести к нарушению ИБ, могут быть как внешние, так и внутренние.

19. Угрозы антропогенного характера могут быть как злоумышленные, так и незлоумышленные.

20. Угрозы ИБ объективно обусловлены наличием уязвимостей в информационной инфраструктуре предприятия, основными из которых являются:

вероятность допуска к работе пользователей, которые не являются лояльными по отношению к предприятию;

наделение пользователей завышенными полномочиями по отношению к компонентам ИС и информационным ресурсам;

неумышленные нарушения работниками правил ИБ;

умышленные нарушения работниками правил ИБ;

технологические сбои в работе компонентов ИС;

наличие незадекларированных возможностей используемых ПС;

уязвимости, возникающие в процессе модернизации компонентов ИС;

ошибки в настройках компонентов ИС;

несвоевременная установка обновлений ПС, влияющих на ИБ.

21. Угрозы ИБ могут возникать через организационно-технологическую инфраструктуру предприятия, которая имеет следующие основные уровни:

физический (линии связи, аппаратные средства и др.);

сетевое оборудование (маршрутизаторы, коммутаторы и др.);

сетевые приложения и сервисы;

операционные системы;

системы управления базами данных.

Глава 5
РЕГЛАМЕНТАЦИЯ ДОПУСКА РАБОТНИКОВ ПРЕДПРИЯТИЯ К ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИОННЫХ РЕСУРСОВ

22. Допуск пользователей к работе с ИС и доступ к ее ресурсам регламентируется следующими аспектами:

основными пользователями информации в ИС являются работники предприятия;

каждый работник имеет индивидуальные права доступа к информации, необходимой ему для выполнения должностных обязанностей;

расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам согласовывается с начальником ОВиА.

23. Работники предприятия несут персональную ответственность за нарушение установленного порядка обработки, хранения и передачи

информации, используемой ими в рамках выполнения должностных обязанностей.

24. Работники предприятия (в том числе вновь принимаемые) должны быть ознакомлены с Политикой под подпись.

25. Изменение количества пользователей и их полномочий в рамках доступа к информации определенных подсистем в ИС производятся согласно Порядку организации доступа к ресурсам информационной системы ОАО «Ратон».

Глава 6
РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА К ИНФОРМАЦИОННОЙ СИСТЕМЕПРЕДПРИЯТИЯ

26. Для входа в ИС работник должен ввести логин и пароль.

27. Организация доступа к ИС осуществляется на основании направляемой в ОВиА заявки подразделения по установленной форме. Специалисты ОВиА осуществляют проверку заявки и определяют техническую возможность, целесообразность и необходимость предоставления доступа к ИС.

28. Параметры входа в сеть, логин и пароль, пользователем не разглашаются. Копии параметров входа в сеть могут содержаться на бумажном носителе в недоступном для посторонних лиц месте.

29. Пользователям запрещается предоставлять доступ к своей учетной записи посторонним лицам.

30. При работе с сетью Интернет пользователям запрещается:

скачивать и устанавливать на компьютер программное обеспечение;

осуществлять деятельность, не имеющую непосредственного отношения к работе и должностным обязанностям;

осуществлять подписку на рассылку информации непроизводственного характера;

сообщать адрес электронной почты в непроизводственных целях;

использовать Интернет в личных целях.

Глава 7
ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ ПРЕДПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

31. Директор предприятия:

определяет цели и задачи СИБ;

принимает решения о совершенствовании СИБ.

32. Начальник ОВиА:

разрабатывает и вносит изменения в локальные правовые акты, регламентирующие вопросы ИБ;

вносит на рассмотрение директору предложения по внедрению наиболее эффективных методов, способов и средств защиты информации;

осуществляет учет информационных ресурсов предприятия, подлежащих защите, и определяет угрозы указанным ресурсам, разрабатывает меры по обеспечению их защиты;

осуществляет анализ внешних и внутренних факторов, обуславливающих возникновение угроз ИБ;

осуществляет выявление и оценку рисков нарушения ИБ, разрабатывает меры по снижению их уровня;

реализует требования ИБ при сопровождении технологических процессов, эксплуатации аппаратно-программных средств;

проводит расследование событий, связанных с инцидентами ИБ, и, в случае необходимости, вносит директору предложения о привлечении к ответственности лиц, нарушивших правила ИБ;

предоставляет и контролирует права доступа работников предприятия к ИС;

контролирует использование сети Интернет, организовывает антивирусную защиту, осуществляет контроль за использованием работниками предприятия сети Интернет и электронной почты;

вносит директору предложения по обеспечению защиты сведений, относящихся к конфиденциальной информации;

организует процессы управления портами ввода-вывода компьютеров и предоставления работникам предприятия прав на использование НЭД;

обеспечивает применение криптографических средств защиты информации и аутентификации участников информационного обмена;

настраивает параметры безопасности компонентов ИС в соответствии с утвержденными стандартами конфигурирования и (или) требованиями ИБ и иными локальными правовыми актами предприятия;

обеспечивает доступ пользователей к компонентам ИС в соответствии с заявками подразделений;

обеспечивает проведение резервного копирования информации в соответствии с установленным порядком;

доводит до работников предприятия требования по ИБ при работе в ИС.

33. Заместители директора, руководители структурных подразделений предприятия обязаны:

выполнять лично и требовать от подчиненных работников выполнение требований Политики, правил работы в ИС, правил обращения с информацией, распространение и (или) предоставление которой ограничено;

оформлять заявки на предоставление работникам предприятия доступа к информационным ресурсам;

сообщать о фактах нарушения работниками правил обращения с информацией, распространение и (или) предоставление которой ограничено, правил работы в ИС, а также об обстоятельствах, которые могут привести к нарушению конфиденциальности информационных ресурсов предприятия.

34. Работники предприятия несут ответственность за исполнение правил ИБ на своем рабочем месте и обязаны:

исключить использование сторонних МНИ (флешки, жесткие диски и т.д.) на рабочих местах без предварительной проверки содержимого на предмет вредоносного ПО, ответственными работниками ОВиА;

использовать информационные ресурсы и технические средства предприятия только для выполнения своих должностных обязанностей;

знать и соблюдать правила ИБ при работе в ИС, правила пользования электронной почтой и сетью Интернет;

сообщать руководителю подразделения и в ОВиА о допущенных фактах нарушения правил обращения с информацией, распространение и (или) предоставление которой ограничено, а также иных обстоятельствах, связанных с нарушениями правил ИБ.

35. Обязанности работников предприятия по выполнению требований ИБ и обращению с информацией, распространение и (или) предоставление которой ограничено, включаются отдельными пунктами в соответствующие разделы трудовых договоров (контрактов) и должностных инструкций.

36. Работникам предприятия запрещается хранение личной информации на информационных ресурсах предприятия (компьютерах и файловых хранилищах) и передавать ее по каналам связи (электронной почте, сети Интернет и др.)

37. Нарушение работниками предприятия требований ИБ является нарушением должностных обязанностей и влечет применение к работникам мер дисциплинарной ответственности.

38. В случае умышленного нарушения работниками предприятия правил ИБ и работы в ИС, повлекшего причинение имущественного или иного ущерба предприятию или его контрагентам, данные действия могут квалифицироваться в соответствии с законодательством Республики Беларусь с применением соответствующих мер наказания.

Глава 8
ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

39. Ознакомление работников ОАО «Ратон» с Политикой ИБ осуществляется через сайт предприятия, на бумажном носителе.

40. При приеме на работу в ОАО «Ратон» проводится ознакомление под подпись принимаемых лиц с положениями Политики ИБ.

41. С целью совершенствования положений Политики ИБ, нормы могут пересматриваться и дополняться в установленном порядке.

Разработчик
Начальник ОВиА _____ 21.06.24 Д.В. Васютин
подпись, дата

СОГЛАСОВАНО:

Зам. директора по
техническому развитию
_____ А.А. Щербин
«24» 06 2024

Специалист по управлению СМК
_____ Е.П. Стрижак
«21» 06. 2024

Юрисконсульт ОПиКР
_____ Д.Ю. Осипкова
«21» 06 2024