

АКЦИОНЕРНОЕ ОБЩЕСТВО
«ЗАРУБЕЖНЕФТЬ»

УТВЕРЖДАЮ
Начальник Управления
информационных технологий
В.В. Курицин

ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ПО ОБЕСПЕЧЕНИЮ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

№ ИН ОБ-09.5-05
РЕДАКЦИЯ 1.00

(взамен Инструкции по организации и проведению работ по защите информации № ИН ОБ-09.5-02
редакция 1.00, утвержденной 12.12.2022)

Идентификатор документа (ELMA Id: 480843eb-18c9-4a39-9f96-19306c5f5a36) Документ подписан		
Владелец сертификата: организация, сотрудник	Сертификат: серийный номер, период действия	Дата и время подписания
КУРИЦИН ВЛАДИМИР ВЯЧЕСЛАВОВИЧ, АО "ЗАРУБЕЖНЕФТЬ"	043CB7AA0034B03FA24031BC8C21EC269E, с 03.07.2023 13:16 по 03.07.2024 13:12	12.03.2024 15:20 Подпись соответствует файлу документа

Москва
2024

ОГЛАВЛЕНИЕ

I. ОБЩИЕ ПОЛОЖЕНИЯ	3
II. ВВЕДЕНИЕ	3
III. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ СВТ	4
3.1. Обязанности пользователя	4
3.2. Обращение со съёмными носителями информации	5
3.3. Работа со средствами криптографической защиты информации и квалифицированной электронной подписью	8
3.4. Обеспечение ИБ при использовании сетей общего пользования	8
3.5. Обеспечение ИБ при работе с электронной почтой	11
3.6. Обеспечение ИБ при работе на СВТ	12
3.7. Выполнение требований парольной политики на СВТ	14
3.8. Обеспечение ИБ при работе с корпоративными мобильными СВТ	15
3.9. Состав и очередность оперативных действий работника при обнаружении признаков компьютерных атак	17
IV. ОТВЕТСТВЕННОСТЬ	19
Приложение № 1	20
Приложение № 2	21
Приложение № 3	24

I. ОБЩИЕ ПОЛОЖЕНИЯ

Наименование документа	Инструкция пользователя по обеспечению информационной безопасности	
Регламентируемый бизнес-процесс	Инструкция частично покрывает бизнес-процесс Об-9.5 «Информационная безопасность» в части установления требований по защите информации при работе пользователей на автоматизированном рабочем месте	
Период действия	Постоянный	
Внешние законодательные требования, требования политик, стратегических документов	<ul style="list-style-type: none"> – Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; – Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; – приказ ФАПСИ от 13.06.2002 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»; – Положение о защите сведений конфиденциального характера в Группе компаний АО «Зарубежнефть»; – Политика информационной безопасности АО «Зарубежнефть»; – Политика управления доступом к ресурсам корпоративной сети 	
Область действия / степень распространения требований на ДО	АО «Зарубежнефть»	Полностью
	ГриД	Полностью
	НиС	Полностью
	Сервисы	Полностью
	Прочие	Полностью
Разработчик документа, должность, ФИО, контакты (e-mail, телефон)	<p>Данник Давид Вахтангович, главный специалист, Управление информационных технологий, т. 30-71, e-mail: ddannik@nestro.ru;</p> <p>Кузнецов Дмитрий Владимирович, руководитель направления, отдел информационной безопасности Центра обслуживания бизнеса АО «Зарубежнефть», т. 84-57, e-mail: dvkuznetsov@nestro.ru</p>	

II. ВВЕДЕНИЕ

2.1. Настоящая Инструкция пользователя по обеспечению информационной безопасности (далее – Инструкция) разработана с целью обеспечения ИБ и предотвращения нарушения устойчивого функционирования информационных систем (далее – ИС),

автоматизированных систем управления и информационно-телекоммуникационных сетей в АО «Зарубежнефть» (далее – Общество) и его дочерних обществах (далее – ДО).

2.2. Настоящая Инструкция устанавливает требования и определяет порядок действий пользователей информационных ресурсов Общества и ДО при эксплуатации корпоративных средств вычислительной техники (далее – СВТ) с целью обеспечения информационной безопасности и соблюдения режима защиты сведений конфиденциального характера, включая персональные данные (далее – СКХ), при её обработке на СВТ в Обществе или ДО.

2.3. Положениями настоящей Инструкции необходимо руководствоваться всем работникам Общества и ДО.

2.4. Положения настоящей Инструкции доводятся до пользователей СВТ Общества и ДО под подпись до предоставления доступа к информационным ресурсам Общества и/или ДО.

2.5. Настоящий документ не распространяется на вопросы защиты информации, составляющей государственную тайну, а также служебной информации ограниченного распространения с пометкой «Для служебного пользования».

III. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ СВТ

3.1. Обязанности пользователя

3.1.1. Знать и выполнять требования действующих нормативных правовых актов Российской Федерации, а также внутренних нормативных документов Общества или ДО, регламентирующих порядок обработки и защиты СКХ и информации, не относящейся к СКХ.

3.1.2. Соблюдать режим допуска в помещение, где проводится обработка СКХ, определенный требованиями пропускного и внутриобъектового режимов, установленных в Обществе или ДО.

3.1.3. Выполнять на СВТ только те процедуры, которые определены для пользователя должностными обязанностями, настоящей Инструкцией и на основании разрешительной системы допуска к ресурсам, программным и техническим средствам ИС.

3.1.4. Знать и строго выполнять правила работы со средствами защиты информации (далее – СЗИ), установленными на СВТ и в ИС.

3.1.5. Хранить в тайне от других свои пароли.

3.1.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.

3.1.7. Обо всех выявленных нарушениях, связанных с ИБ, сообщениях электронной почты, вызывающих подозрения пользователя, а также для получения консультаций по вопросам ИБ необходимо обращаться в отдел информационной безопасности Центра

обслуживания бизнеса АО «Зарубежнефть» (далее – ОИБ) посредством направления сообщения на адрес cib@nestro.ru или по телефону +7 (846) 276-26-00 доб. 8889. В случае переадресации сообщения посредством электронной почты необходима отметка о подозрении на наличие вредоносного программного обеспечения (далее – ПО) во вложении или фишинговых ссылок.

3.1.8. Принимать меры по реагированию в случае возникновения внештатных и аварийных ситуаций на СВТ с целью уменьшения либо ликвидации их последствий.

3.1.9. Предоставлять работнику(-ам) Общества и/или ДО, осуществляющему(-им) установленным Инструкцией по мониторингу событий и управлению инцидентами информационной безопасности в АО «Зарубежнефть» и его дочерних обществах порядком расследование инцидента ИБ:

- запрашиваемую информацию;
- письменные объяснения относительно инцидента;
- доступ в помещения Общества или ДО, в том числе к своему рабочему месту, а также к СВТ, закрепленным за работником.

3.1.10. При отсутствии визуального контроля за СВТ доступ к операционной системе (далее – ОС) должен быть заблокирован.

3.2. Обращение со съёмными носителями информации

3.2.1. В целях предотвращения разглашения, утечки или утраты информации в Обществе и ДО применяются меры защиты съёмных носителей информации, изложенные в данном разделе Инструкции.

3.2.2. Съёмные носители информации делятся на следующие категории:

- конфиденциальные съёмные носители информации, предназначенные для обработки информации, содержащей СКХ, в соответствии с Перечнем сведений конфиденциального характера АО «Зарубежнефть», внутренними нормативными документами ДО;
- прочие съёмные носители информации, предназначенные для обработки не конфиденциальной информации, используемой в текущей деятельности.

3.2.3. Порядок учёта, маркировки, выдачи и работы со съёмными носителями информации, предназначенными для обработки СКХ, осуществляется в соответствии с Положением о защите сведений конфиденциального характера в Группе компаний АО «Зарубежнефть» (далее – Положение о защите СКХ), Инструкцией по конфиденциальному делопроизводству в АО «Зарубежнефть», внутренними нормативными документами ДО.

3.2.4. Для выполнения своих трудовых обязанностей или поставленной руководителем задачи работник может на постоянной основе на выданном ему СВТ использовать съёмный носитель информации, не содержащей СКХ. Выдачу данных съёмных носителей информации

в Обществе или ДО осуществляют работники структурного подразделения, ответственного за материально-техническое обеспечение пользователей.

3.2.5. Прочие съёмные носители информации, не содержащей СКХ, подлежат учету в журнале учета съёмных носителей информации по форме, определенной настоящей Инструкцией (Приложение № 1). Учет и маркировка прочих съёмных носителей информации осуществляется работниками, структурных подразделений Общества или ДО, ответственных за поддержку пользователей (в АО «Зарубежнефть» – Группа поддержки пользователей Центра обслуживания бизнеса).

3.2.6. Учет съёмных носителей информации основывается на учетных номерах, в качестве которых должны использоваться серийные номера съёмных носителей информации, присвоенные производителями, или номера инвентарного учета.

3.2.7. Маркировка прочих съёмных носителей информации осуществляется путем проставления работниками, структурных подразделений Общества или ДО, ответственных за поддержку пользователей, на корпусе носителя уникального идентификатора съёмного носителя информации (vid&pid) или учетного номера, или иной информации, позволяющей идентифицировать носитель.

3.2.8. Регистрация всех съёмных носителей, содержащих и не содержащих СКХ, для работы на СБТ осуществляется работниками структурного подразделения Общества или ДО, ответственными за обеспечение ИБ (в АО «Зарубежнефть» – ОИБ), путем внесения уникального идентификатора съёмного носителя информации (vid&pid), в систему контроля утечки конфиденциальной информации (при ее отсутствии – в иных СЗИ) с обеспечением блокирования записи информации на незарегистрированные съёмные носители информации. Уникальный идентификатор съёмного носителя информации (vid&pid) передаётся в ОИБ для регистрации работниками, осуществляющими учет съёмных носителей информации.

3.2.9. В Обществе и ДО допускается применение только учтённых съёмных носителей информации.

3.2.10. Применение незарегистрированных съёмных носителей информации в Обществе и ДО запрещено.

3.2.11. Перед началом работы со съёмным носителем информации осуществить проверку носителя на предмет отсутствия компьютерных вирусов.

3.2.12. При отсутствии дальнейшей необходимости в использовании съёмного носителя информации, уход в длительный отпуск, увольнение или перевод работника на другую должность съёмный носитель информации подлежит передаче структурному подразделению, осуществляющему его учет.

3.2.13. Работнику необходимо регулярно проводить (не реже 1 раза в месяц) ревизию СКХ, размещенных на всех числящихся за ним конфиденциальных съёмных носителях информации, на предмет наличия на носителе СКХ, цель обработки которых была достигнута.

3.2.14. По достижению целей обработки СКХ вся информация на конфиденциальном съёмном носителе должна быть удалена без возможности её восстановления средствами гарантированного уничтожения информации. При невозможности удаления СКХ машинные носители информации подлежат уничтожению (физическому разрушению).

3.2.15. Съёмные носители информации, пришедшие в негодность или с истекшим сроком эксплуатации, а также однократного применения также подлежат уничтожению.

3.2.16. Для удаления информации или для физического уничтожения съёмного носителя информации работник передаёт его структурному подразделению, осуществляющему учет съёмных носителей информации.

3.2.17. Для хранения съёмных носителей информации должны использоваться специально оборудованные хранилища (сейфы, шкафы, запираемые ящики), исключающие возможность несанкционированного доступа к ним посторонних лиц.

3.2.18. При утрате съёмного носителя информации работник обязан незамедлительно поставить в известность непосредственного руководителя, Управление информационных технологий АО «Зарубежнефть» (далее – УИТ) или ответственных за информационные технологии работников ДО.

3.2.19. По каждому факту утраты конфиденциального съёмного носителя информации проводится внутреннее расследование/проверка в соответствии с Инструкцией по конфиденциальному делопроизводству в АО «Зарубежнефть», внутренними нормативными документами ДО.

3.2.20. При работе со съёмными носителями информации запрещено:

- несанкционированно подключать съёмные носители информации к СБТ;
- использовать корпоративные съёмные носители информации Общества и ДО в личных целях, в том числе для удаленной работы на личных АРМ;
- осуществлять обработку СКХ на съёмных носителях информации, не предназначенных для этой цели;
- использовать конфиденциальные съёмные носители информации, для хранения СКХ, которые не требуются работнику для выполнения им своих трудовых обязанностей или для выполнения поставленной руководителем задачи;
- осуществлять несанкционированную передачу СКХ третьим лицам.

3.3. Работа со средствами криптографической защиты информации и квалифицированной электронной подписью

3.3.1. Работники Общества или ДО, имеющие в обращении квалифицированную электронную подпись (далее – КЭП), обеспечивают сохранность КЭП, выданной им в соответствии с пунктом 2.1 Инструкции об использовании квалифицированной электронной подписи в Группе компаний АО «Зарубежнефть».

3.3.2. Хранение средств криптографической защиты информации (далее – СКЗИ) и КЭП, а также эксплуатационной и технической документации к ним осуществляется в запираемых шкафах (ящиках, хранилищах, сейфах), исключающих бесконтрольный доступ к ним.

3.3.3. Работникам Общества или ДО при работе с СКЗИ запрещается:

- оставлять без контроля СВТ, на которых эксплуатируется СКЗИ;
- вносить какие-либо изменения в ПО СКЗИ;
- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое ключевых носителей или передавать сами носители третьим лицам, к ним не допущенным;
- записывать на ключевые носители постороннюю информацию;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ;
- хранить закрытые ключи КЭП на жестком диске автоматизированного рабочего места (далее – АРМ).

3.4. Обеспечение ИБ при использовании сетей общего пользования

3.4.1. По умолчанию доступ работников Общества и ДО к Интернет-ресурсам с их АРМ заблокирован. Для получения разрешения работы с определенными Интернет-ресурсами, доступ к которым необходим для выполнения должностных обязанностей работника, оформляется обоснованная заявка в АСПП, которая согласовывается с УИТ и ОИБ.

3.4.2. Доступ работников Общества или ДО к Интернет-ресурсам, которые запрещены законодательством Российской Федерации и (или) могут представлять угрозу ИБ, включая материалы террористического, националистического, расистского, развлекательного, религиозного, сексуального и другого характера, запрещен.

3.4.3. При работе в информационно-телекоммуникационной сети Интернет работник Общества или ДО обязан:

- использовать информационно-телекоммуникационную сеть Интернет только в целях исполнения своих должностных обязанностей;
- соблюдать принципы делового общения и этикета, пользуясь Интернет-ресурсами с АРМ;
- при обнаружении нетипичных действий со стороны Интернет-ресурса (автоматическом открытии множества окон в браузере, предложении оптимизировать производительность,

обновить ПО, начать лечение зараженного компьютера, объявлении о выигрыше денежного приза и т.п.), не переходя по ссылкам, незамедлительно покинуть данный ресурс.

3.4.4. При работе в информационно-телекоммуникационной сети Интернет работнику Общества или ДО запрещено¹:

- предпринимать самостоятельные действия по устранению неполадок подключения к информационно-телекоммуникационной сети Интернет при их возникновении;
- использовать предоставленный доступ к информационно-телекоммуникационной сети Интернет для организации доступа к ней других лиц;
- осуществлять работу в информационно-телекоммуникационной сети Интернет с использованием учетных записей с административными правами доступа. При производственной необходимости доступ в информационно-телекоммуникационную сеть Интернет с использованием учетной записи с административными правами доступа оформляется в соответствии с Политикой управления доступом к ресурсам корпоративной сети, внутренними нормативными документами ДО, с развернутым обоснованием необходимости доступа и обязательным согласованием с заместителем Генерального директора, курирующим вопросы ИБ в Обществе, или с заместителем Генерального директора ДО, на которого возложены функции обеспечения ИБ в ДО;
- использовать Интернет-ресурсы для распространения информации, запрещенной законодательством Российской Федерации, включая материалы террористического, националистического, расистского, сексуального, религиозного, развлекательного и другого характера, а также информацию, оскорбляющую честь и достоинство других лиц;
- использовать доступ в информационно-телекоммуникационную сеть Интернет для личной переписки (как по электронной почте, так и другими программными средствами с использованием информационно-телекоммуникационной сети Интернет);
- использовать доступ в информационно-телекоммуникационную сеть Интернет для работы со следующими типами Интернет-ресурсов:
 - публичные сервисы электронной почты (например, mail.ru, yandex.ru, mail.google.com и т.д.);
 - файлообменные сервисы (например, Anonfiles.com, Dropmefiles.com);
 - облачные хранилища (например, onedrive.com, disk.yandex.ru, dropbox.com, drive.google.com и т.д.);
 - пиринговые (p2p) сети (например, BitTorrent, eMule и т.д.);

¹ Наличие технической возможности доступа к указанным в настоящем разделе категориям Интернет-ресурсов, либо возможности совершения запрещенных действий не дает работнику права их совершать.

- средства анонимного доступа к Интернет-ресурсам, анонимайзеры (например, Tor, I2P, OpenVPN, веб-прокси и т.д.);
- социальные сети (например, Facebook.com, vk.com, ok.ru, Instagram, Tik-tok, Pinterest, Reddit и т.д.);
- средства мгновенного обмена сообщениями и чаты (например, Skype, WhatsApp, Viber, Telegram, Signal, Threema, ICQ, IRC и т.д.);
- удаленный доступ СБТ, находящимися за пределами корпоративной сети, способами, выходящими за рамки утвержденных проектных решений (например, с использованием программ удаленного доступа к компьютеру, в том числе TeamViewer, Ammy Admin, RMS, Radmin, Supremo и т.д.);
- игровые, развлекательные сайты и прочие ресурсы, не предназначенные для выполнения должностных обязанностей;
- публиковать в информационно-телекоммуникационной сети Интернет, а также передавать через информационно-телекоммуникационную сеть Интернет способами, отличающимися от утвержденных в Положении о защите СКХ и иных внутренних нормативных документах Общества или ДО:
 - СКХ;
 - исходные коды разработанных и разрабатываемых в интересах Общества и ДО программ, скриптов, макросов и т.д., в том числе на сайтах Github.com, Gitlab.com и других системах управления версиями;
 - специально преобразованную (зашифрованную) информацию, в том числе архив с паролем (за исключением информации, разрешенной для передачи в зашифрованном виде в соответствии с утвержденными нормативными или организационно-распорядительными документами, или с принятыми техническими решениями Общества или ДО, а также эксплуатационными документами на аппаратно-программные средства, используемые в рамках заключенных с контрагентами договоров);
- загружать из информационно-телекоммуникационной сети Интернет, запускать (открывать) исполняемые файлы (с расширением .exe, .com, .bat, .cmd, .cpl, .js, .vs, .lnk, .msi, .pif, .scr, .vbs, .wsf, .class, .ps1, .sh, .deb, .tar.gz и т.д.), файлы без расширений, файлы неизвестного/сомнительного содержания, в т. ч. содержащиеся в архивах, если это не предусмотрено должностными обязанностями;
- публиковать, передавать, запрашивать и использовать любую информацию или ПО, которые заведомо содержат или могут содержать в себе вредоносное содержимое;
- использовать корпоративный адрес электронной почты для регистрации и публикации на Интернет-ресурсах (на досках объявлений, форумах, гостевых книгах, интернет-магазинах и т. п.), за исключением случаев исполнения должностных обязанностей;

- использовать пароли, применяемые для доступа к Интернет-ресурсам, в качестве паролей доступа объектам защиты Общества и ДО.

3.5. Обеспечение ИБ при работе с электронной почтой

3.5.1. Доступ к корпоративной электронной почте предоставляется работникам только в целях исполнения трудовых функций.

3.5.2. Вся служебная переписка должна осуществляться только с использованием персонального адреса корпоративной электронной почты или адресов корпоративной электронной почты, предназначенных для массовых рассылок и оповещений.

3.5.3. Работник должен проверять вложения в сообщениях электронной почты на наличие исполняемых файлов (.exe, .com, .bat, .cmd, .cpl, .js, .vs, .lnk, .msi, .pif, .scr, .vbs, .wsf, .class, .ps1, .sh, .deb, .tar, .gz и т.д.), при их наличии - не запускать исполняемый файл и сообщить о получении такого письма в УИТ и ОИБ с обязательным указанием вредоносного вложения, а не простой пересылкой сообщения.

3.5.4. При работе с электронной почтой запрещено:

- осуществлять массовую и адресную рассылку информации, не связанной со служебной необходимостью;
- направлять СКХ без применения СКЗИ по открытым (незащищенным) каналам передачи данных, в том числе через сети общего пользования и информационно-телекоммуникационную сеть Интернет;
- использовать любые другие сервисы электронной почты кроме корпоративных, если иное не предусмотрено исполнением должностных обязанностей;
- переходить по внешним ссылкам, указанным в электронных письмах, в случае если получение такого письма не связано с выполнением должностных обязанностей;
- регистрировать учетные записи, профили на сторонних Интернет-ресурсах (включая социальные сети) с указанием корпоративного адреса электронной почты, за исключением случаев, связанных с выполнением должностных обязанностей;
- осуществлять пересылку СКХ на сторонние (не корпоративные) адреса электронной почты;
- осуществлять рассылку сообщений, содержащих игры, развлекательное и другое ПО, не имеющее отношения к выполнению должностных обязанностей, личные фотографии и видеоролики;
- осуществлять рассылку сообщений, зараженных вирусами или при подозрении о вирусной активности на СБТ;
- осуществлять рассылку сообщений рекламного или не относящегося к работе содержания, людям, которые не давали своего согласия на их получение (SPAM).

3.5.5. Перед отправкой сообщений электронной почты необходимо проверить адреса получателей письма, а также наличия СКХ во вложениях и обоснованность её отправки.

3.5.6. При получении подозрительного письма с сомнительным содержанием и/или от неизвестного отправителя с вложением, работникам запрещено открывать это письмо, а в случае его открытия – не открывать вложения, не переходить по указанным ссылкам и сообщить в ОИБ и УИТ о факте получения такого письма.

3.6. Обеспечение ИБ при работе на СВТ

3.6.1. При работе на СВТ работник обязан:

- использовать СВТ только для выполнения должностных обязанностей;
- использовать только свои учетные записи для доступа к информационным ресурсам Общества и ДО;
- незамедлительно проинформировать непосредственного руководителя, ОИБ и УИТ при выявлении нарушений требований ИБ, связанных с эксплуатацией СВТ, в том числе другими лицами;
- по окончании сеанса работы на СВТ или при необходимости оставления рабочего места заблокировать экран СВТ нажатием на компьютерной клавиатуре набора клавиш Ctrl+Alt+Del и далее – кнопки «Заблокировать» («Lock Workstation») или Win+L, по окончании рабочего времени и/или при покидании рабочего места на длительный срок (убытие в отпуск, командировку и т.д.) – выключить СВТ (при отсутствии иных указаний);
- немедленно уведомлять УИТ о случаях сбоев антивирусного ПО (появления сообщений об ошибках, об устаревших антивирусных базах), с описанием возникшей проблемы. При возможности, к обращению необходимо приложить снимок экрана, иллюстрирующий возникшую проблему.

При обработке СКХ:

- руководствоваться нормами Положения о защите СКХ и Инструкции по конфиденциальному делопроизводству в АО «Зарубежнефть» или ДО;
- осуществлять обработку СКХ на СВТ с внедрённым комплексом СЗИ;
- осуществлять работу и хранение СКХ на:
 - а) съёмном носителе информации, учтённом и выданном Управлением корпоративной безопасности АО «Зарубежнефть» (далее – УКБ);
 - б) информационных ресурсах, предназначенных для обработки (хранения) СКХ;
 - в) информационных системах, в которых разрешена обработка СКХ;
- не допускать ситуации, в которой лица, не допущенные к обработке СКХ, могут с ней ознакомиться;
- хранить СКХ обособленно от информации, доступ к которой предоставляется широкому кругу лиц;
- использовать для защиты СКХ, передаваемой по каналам связи за пределы корпоративной сети, СКЗИ (например: VipNet, Континент-АП и т.п.);

- не размещать СКХ в публичных социальных сетях, облачных хранилищах, файлообменных сервисах в сети Интернет.

3.6.2. При работе на СБТ работнику запрещено:

- эксплуатировать СБТ при отключенных или неустановленных средствах антивирусной защиты;
- оставлять рабочее место без блокирования экрана СБТ;
- срывать пломбы или печати, вскрывать корпус персонального компьютера, осуществлять самостоятельную сборку и разборку СБТ;
- использовать уязвимости и недокументированные возможности установленного ПО;
- вносить изменения в аппаратную и программную конфигурацию СБТ;
- хранить личную, не имеющую отношения к выполнению должностных обязанностей, информацию на СБТ и сетевых ресурсах;
- производить загрузку СБТ с внешних носителей;
- получать доступ к BIOS / UEFI персонального компьютера;
- использовать СБТ с локальными учетными записями;
- препятствовать работе СЗИ или пытаться обходить их;
- самостоятельно подключать к СБТ периферийные и внешние устройства, в том числе:
 - принтеры, сканеры и многофункциональные устройства;
 - модемы и адаптеры связи;
 - мобильные телефоны, планшеты и другие подобные устройства;
 - личные носители информации;
- оставлять корпоративные мобильные СБТ (ноутбук, смартфон, планшет) в общедоступных местах без присмотра;
- осуществлять подключение (проводное или беспроводное) к СБТ личных мобильных устройств (смартфон, планшет, модем или другие внешние устройства), в том числе с целью зарядки;
- производить самостоятельное удаление / установку ПО на СБТ, включая СЗИ;
- прерывать процесс загрузки ОС, выполняемый по умолчанию и использовать альтернативные режимы загрузки ОС;
- передавать пароли своих учетных записей другим пользователям;
- хранить в открытом доступе логин и пароль;
- передавать в открытом виде СКХ по незащищенным каналам передачи данных;
- использовать ПО и/или оборудование Общества или ДО с целью извлечения личного дохода;

- использовать недокументированные свойства и ошибки в ПО или в настройках СЗИ Общества или ДО, которые могут привести к нарушению их штатной работы, отключению, повышению полномочий пользователя или несанкционированному доступу к данным;
- обрабатывать данные, отнесенные к служебной информации ограниченного распространения с пометкой «Для служебного пользования» или к информации, составляющей государственную тайну.

3.7. Выполнение требований парольной политики на СВТ

3.7.1. Пользователи корпоративной сети должны производить смену своих паролей к учетной записи на СВТ не реже, чем раз в 90 дней. Новые пароли не должны совпадать с использовавшимися ранее. Пользователям запрещается предпринимать какие-либо действия по получению (раскрытию) паролей других пользователей.

3.7.2. Учетная запись пользователя блокируется после 5 неудачных попыток введения пароля. Разблокировка учетной записи осуществляется в соответствии с пунктом 5.1 Политики управления доступом к ресурсам корпоративной сети.

3.7.3. Для доступа к различным информационным ресурсам и системам пользователи должны иметь строго различные пароли, не вычисляемые один из другого, а также не использовать один и тот же пароль для доступа к внутренним данным локальной сети и при использовании внешних информационных систем (например, Интернет-ресурсов).

3.7.4. Требования к сложности паролей.

Выбираемый пользователем пароль должен одновременно отвечать приведенным ниже требованиям:

- содержать не менее 12 символов;
- содержать цифры (0-9);
- содержать символы в верхнем и нижнем регистрах;
- содержать специальные символы (\$, #, % и т.д.);
- запрещено использовать имя своей учетной записи в пароле;
- не являться персональной информацией (имена членов семьи, адреса, телефоны, даты рождения и т.п.).

В случае невозможности применения указанных в данном пункте Инструкции требований для прикладного или системного ПО, указанные требования применяются с учетом технических возможностей для конкретного СВТ, до момента их приведения в соответствие с указанными выше требованиями. До этого необходимо придерживаться наиболее жесткого ограничения.

3.7.5. Пользователи обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей. Запрещается:

- сообщать свой пароль кому-либо, включая коллег, руководителей и специалистов подразделений, осуществляющих техническую поддержку, по телефону, по электронной почте или какими-либо иными средствами;
- хранить пароли в доступной для чтения форме в командных файлах, сценариях автоматической регистрации, программных макросах, на компьютерах с неконтролируемым доступом, а также в иных местах, где неуполномоченные лица могут получить к ним доступ;
- записывать пароли и оставлять эти записи в местах, где к ним могут получить доступ неуполномоченные лица. Например, наклеивать листочки с записанными паролями на монитор, или складывать их в ящик стола. Допускается хранение паролей в письменном виде в личном сейфе;
- произносить свой пароль вслух в присутствии других лиц;
- использовать в качестве паролей последовательность повторяющихся символов и их комбинации (например, «1114444», «aaaaaУУУ»), либо комбинаций символов, набираемых в закономерном порядке на клавиатуре (например, «QAZwsx», «1йфя2цыч», «qwerty1234»), а также любых названий месяцев года в различных языковых раскладках клавиатуры (например, «Июнь», «В.ум», «Декабрь», «Ltrf,fhm», «Январь_2022»);
- использовать предустановленные заводские пароли и пароли по умолчанию;
- сохранять пароли в браузере и программах для осуществления подключения.

3.7.6. В случаях, когда кто-либо требует от пользователя раскрытия пароля, пользователь должен отказать в исполнении требования, сославшись на Политику управления доступом к ресурсам корпоративной сети или настоящую Инструкцию.

3.7.7. Пароль должен быть немедленно изменен пользователем, если имеются основания полагать, что данный пароль стал известен кому-либо еще кроме самого пользователя.

3.8. Обеспечение ИБ при работе с корпоративными мобильными СВТ

3.8.1. УИТ разрабатывает и согласовывает с ОИБ технические требования на подключение к информационно-телекоммуникационной инфраструктуре корпоративных мобильных СВТ (ноутбук, планшет, смартфон).

3.8.2. Выдача всех корпоративных мобильных СВТ должна проводиться в соответствии с Политикой управления доступом к ресурсам корпоративной сети, путем подготовки соответствующей заявки в АСПП, согласованной руководителем структурного подразделения, в котором работает пользователь, руководителем УИТ, с последующим принятием корпоративных мобильных СВТ на техническую эксплуатацию и сопровождение Группы поддержки пользователей Центра обслуживания бизнеса АО «Зарубежнефть» (в ДО – подразделение, осуществляющее поддержку пользователей ДО) или организацией, на

которую функции по технической эксплуатации и сопровождению СВТ возложены по договору.

3.8.3. В некоторых случаях (проведение презентаций, выезд в командировку в место, где необходимо использовать корпоративное мобильное СВТ, решение нетиповых задач) работник может оформить заявку на временное получение корпоративного мобильного СВТ. По достижению цели использования такого мобильного СВТ перед сдачей пользователь обязан удалить все записанные им файлы (проекты документов, материалы презентаций и т.п.) с мобильного СВТ.

3.8.4. При работе с корпоративными мобильными СВТ пользователи обязаны:

- обеспечить соблюдение требований ИБ, определённых настоящей Инструкцией и иными внутренними нормативными документами Общества или ДО при обработке СКХ, удаленном доступе к информационным ресурсам Общества или ДО, доступе к внешним машинным носителям информации, доступе к информационно-телекоммуникационной сети Интернет, подключении к корпоративной сети;
- по запросу уполномоченного работника или организации, на которую возложены функции по технической эксплуатации и сопровождению СВТ, предоставлять в указанный в запросе срок корпоративное мобильное СВТ для проведения работ по технической эксплуатации и сопровождению, в том числе по обновлению антивирусного ПО и политик безопасности, установке обновлений безопасности системного и прикладного ПО, установке актуальных версий ПО, смене паролей BIOS / UEFI и административных учетных записей;
- при отсутствии производственной необходимости, увольнении или переводе работника в другое структурное подразделение Общества или ДО сдать корпоративное мобильное СВТ структурному подразделению Общества или ДО, выдавшему СВТ (при этом рабочая информация, хранившаяся на корпоративном мобильном СВТ локально, должна быть, по возможности, удалена работником до его сдачи);
- исключить возможность использования корпоративных мобильных СВТ посторонними лицами;
- незамедлительно сообщить об утере/краже корпоративного мобильного СВТ непосредственному руководителю, в ОИБ, УИТ и УКБ (в ДО – руководителям подразделений ИБ и безопасности).

3.8.5. Использование административных учетных записей для выполнения повседневных задач на корпоративных мобильных СВТ запрещено.

3.8.6. Работнику запрещено самостоятельно осуществлять техническую эксплуатацию и сопровождение выданного ему корпоративного мобильного СВТ.

3.8.7. Работники, осуществляющие техническую эксплуатацию и сопровождение корпоративных мобильных СВТ, обязаны обеспечить соблюдение требований ИБ в соответствии с нормативными документами Общества или ДО.

3.8.8. На корпоративных мобильных СВТ работником Общества или ДО, осуществляющим функции по технической эксплуатации и сопровождению СВТ, или организацией, на которую функции по технической эксплуатации и сопровождению СВТ возложены договором, должно быть установлено антивирусное ПО с актуальным набором сигнатур.

3.8.9. Для доступа к ресурсам корпоративной сети использовать многофакторную аутентификацию (логин и пароль персональной рабочей учетной записи, генератор одноразовых паролей, при установлении защищенного соединения (VPN), СЗИ от несанкционированного доступа и USB-токен, статический ip-адрес).

3.8.10. На корпоративном мобильном СВТ должны использоваться пароли, удовлетворяющие требованиям парольной политики Общества или ДО.

3.8.11. Обработка СКХ на корпоративных мобильных СВТ, осуществляется только после оснащения последних комплексом СЗИ и выполнения иных требований по её защите, установленных в Обществе или ДО.

3.9. Состав и очередность оперативных действий работника при обнаружении признаков компьютерных атак

3.9.1. При обнаружении предположительных или явных признаков компьютерных атак на СВТ с использованием вредоносной программы, например:

- неожиданное появление на экране монитора сообщений о шифровании рабочих файлов на СВТ, о требовании перечислить денежные средства, в том числе в качестве выкупа за обратную расшифровку, и тому подобные;
- замена стартовой страницы Интернет-браузера при каждом старте системы, периодическое самопроизвольное открытие окон Интернет-браузера, самовольное изменение расширения файлов;
- обнаружение подключенного к USB-порту СВТ машинного носителя информации (flash-накопителя, внешнего жесткого диска, мобильного телефона), который пользователь не подключал, т.е. неизвестного происхождения;
- наличие в разделе «Отправленные» писем и/или получение большого количества отчётов с сообщениями о результатах доставки писем, которые пользователь не отправлял.

Работник Общества или ДО обязан незамедлительно выполнить следующие действия:

- а) приостановить работу без перезагрузки СВТ;
- б) отсоединить от корпуса СВТ шнур подключения к корпоративной сети;

в) незамедлительно поставить в известность о факте обнаружения признаков компьютерной атаки ОИБ, УИТ, а также непосредственного руководителя;

г) ожидать дальнейших указаний от ОИБ, УИТ.

3.9.2. При обнаружении предположительных или явных признаков компьютерных атак, проводимых посредством фишинговых (мошеннических) электронных писем и/или телефонных звонков, например:

- отправитель письма или телефонный собеседник требует от пользователя незамедлительных действий, т.к. иначе что-то случится, например, расчетный счет заблокируют или будет выписан штраф. Злоумышленники используют «ситуацию срочности», чтобы пользователь совершил ошибку и у него было как можно меньше времени на размышление;
- пользователь получил электронное письмо, которого не ждал, например, от известной организации, с которой нет договорных отношений, пришло электронное письмо с вложением или ссылкой на архив с подробностями заказа. В письме может также говориться о том, что во вложении информация о просроченном кредите, деталях увольнения пользователя, повышения заработной платы, внезапного выигрыша или штрафа из налоговой инспекции;
- в письме не указывается имя пользователя, а используется общее обращение: «Уважаемый Клиент». Важно помнить, что большинство работников компаний-партнеров знают имена своих клиентов и используют эти сведения в деловой переписке;
- отправителем письма или позвонившим запрашивается от пользователя конфиденциальная информация, например, имя учетной записи, пароль или номер кредитной карты, информация из корпоративного телефонного справочника;
- пользователь получил письмо от своего знакомого или коллеги, но текст или смысл письма вызывает подозрения в том, что знакомый или коллега является автором письма. При уточнении выясняется, что знакомый или коллега данное письмо не писал.

Работник Общества или ДО обязан незамедлительно выполнить следующие действия:

а) не открывать вложения и не переходить по ссылкам в тексте письма с признаками фишинга;

б) завершить телефонный разговор, не сообщая по телефону неизвестным лицам конфиденциальную информацию;

в) переслать как вложение или скриншот (фотографию экрана СБТ) на почтовый адрес ОИБ поступившие письма подозрительного содержания. В теме письма указать предупреждение, например, «Внимание! Возможно, вирус во вложении!»;

г) не удалять письмо до получения инструкций от ОИБ.

IV. ОТВЕТСТВЕННОСТЬ

4.1. Работники Общества и ДО несут персональную ответственность за выполнение возложенных на них в соответствии с настоящей Инструкцией обязанностей.

4.2. Работники Общества или ДО, не выполняющие требования настоящей Инструкции, могут быть привлечены к ответственности в соответствии с применимым законодательством.

4.3. Ответственность за обеспечение ИБ и соблюдение режима ИБ лицами, не являющимися работниками Общества или ДО, при проведении ими работ на объектах информатизации Общества или ДО определяется гражданско-правовыми договорами и соглашениями, заключаемыми с этими лицами.

Приложение № 1
к Инструкции пользователя по
обеспечению информационной
безопасности

**Журнал
учета съемных носителей информации**

№ п/п	Учетный номер съемного носителя информации/ серийный номер	Тип/ёмкость съемного носителя информации	Место установки (использования) / дата установки	Работник, получивший съемный носитель (ФИО)	Расписка в получении (подпись, дата)	Расписка о возврате съемного носителя информации (ФИО, подпись, дата)	Сведения об уничтожении съемного носителя стирании информации (подпись, дата)
1	2	3	4	5	6	7	8

Начат «__» _____ 20__ г.

Ответственный за ведение журнала: _____ /ФИО, должность/

СПИСОК СОКРАЩЕНИЙ, ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

Термины и определения:

Термин	Определение
Автоматизированное рабочее место	Рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных с целью получения информации, обеспечивающей поддержку принимаемых им решений при выполнении профессиональных функций
Аутентификация	Совокупность мероприятий по проверке лица на принадлежность ему идентификатора (идентификаторов) посредством сопоставления его (их) со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению правомерности владения лицом идентификатором (идентификаторами) посредством использования аутентифицирующего (аутентифицирующих) признака (признаков) в рамках процедуры аутентификации, в результате чего лицо считается установленным
Вредоносная программа	Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы
Идентификация	Совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с уникальным обозначением (уникальными обозначениями) сведений о лице, необходимым для определения такого лица
Информационно – телекоммуникационная сеть	Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием СВТ
Информационная система	Совокупность программно-технических и других средств, используемых для хранения, обработки и передачи информации, с целью решения бизнес-задач подразделений Общества
Ключевой носитель	Физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного

Термин	Определение
	использования (магнитная лента, дискета, компакт-диск, Data Key, Smart Card, Touch Memory и т.п.)
Компьютерная атака	Целенаправленное несанкционированное воздействие на информацию, на ресурс информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств
Объекты защиты	Информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети
Пользователь	Работник, которому разрешено выполнять с использованием СВТ некоторые действия (операции) по обработке информации, в том числе СКХ, в информационных системах и информационных ресурсах, использовать результаты их функционирования
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (в т.ч. автоматизированные рабочие места, ноутбуки, планшеты и т.п.)
Съемные носители	Флеш-накопители, внешние жесткие диски, CD-,DVD диски и иные отчуждаемые устройства
Учетная запись пользователя	Совокупность сведений о пользователе, которая включает в себя имя пользователя и его уникальный идентификатор (далее – логин), однозначно идентифицирующий данного пользователя в ОС (сети, базе данных, приложении и т.п.) и служащий для определения пользовательских полномочий по доступу к ресурсам. Учётная запись создается системным администратором при регистрации пользователя в ОС компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.
Электронная подпись	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

Список сокращений:

Сокращение	Полное наименование
АРМ	Автоматизированное рабочее место
АСПП	Автоматизированная система поддержки пользователей
ДО	Дочернее общество АО «Зарубежнефть»
ИБ	Информационная безопасность
Инструкция	Инструкция пользователя по обеспечению информационной безопасности

Сокращение	Полное наименование
ИС	Информационная система
КЭП	Квалифицированная электронная подпись
Мобильные СВТ	Мобильное средство вычислительной техники (ноутбук, планшет, смартфон)
Общество	АО «Зарубежнефть»
ОИБ	Отдел информационной безопасности Центра обслуживания бизнеса АО «Зарубежнефть»
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
СВТ	Средство вычислительной техники
СЗИ	Средства защиты информации
СКЗИ	Средства криптографической защиты информации
СКХ	Сведения конфиденциального характера
УИТ	Управление информационных технологий АО «Зарубежнефть»

**Ключевые вопросы к Инструкции пользователя
по обеспечению информационной безопасности**

1. Кого необходимо информировать обо всех выявленных нарушениях, связанных с ИБ?
2. Разрешено ли использование личных съёмных носителей информации на СВТ?
3. Что запрещено пользователю СКЗИ?
4. В каких случаях съёмные носители информации подлежат уничтожению?
5. Как часто должен меняться пароль к учётной записи на СВТ?