АКЦИОНЕРНОЕ ОБЩЕСТВО
«ТАИФ-НК»

УЭБОиР-П-05-23

ПОЛОЖЕНИЕ ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АО «ТАИФ-НК»

Введено в действие
Приказом № _____ от _____

с _____

Срок действия

до _____

г. Нижнекамск

УТВЕРЖДАЮ
Генеральный директор
АО «ТАИФ-НК»
_____ М.А. Новиков

«_____» _____ 2023 г.

УЭБОИР-П-05-23 ПОЛОЖЕНИЕ ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АО «ТАИФ-НК»

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящее положение устанавливает единый порядок и основные требования по обеспечению информационной безопасности при работе на персональных автоматизированных рабочих местах в информационных и автоматизированных системах АО «ТАИФ-НК» в соответствии с требованиями законодательства Российской Федерации, включая:

– Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

– Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

– Локальные нормативные документы Общества в области обеспечения информационной безопасности.

1.2. Действие настоящего положения распространяется на всех работников АО «ТАИФ-НК», в том числе временных, при условии доступа к информационным и автоматизированным ресурсам, а также на третьих лиц (партнеров, потребителей, поставщиков, консультантов), получающих доступ к информации в рамках договорных отношений.

1.3. Настоящее положение обязательно для исполнения всеми структурные подразделениями АО «ТАИФ-НК», в которых осуществляется автоматизированная обработка информации, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение функционирования информационных и автоматизированных систем АО «ТАИФ-НК».

2 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированное рабочее место – автоматизированное рабочее место пользователя (персональный компьютер с прикладным и системным программным обеспечением) для выполнения определенной производственной задачи.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированная система управления технологическими процессами – совокупность информационных технологий и технических средств, а также обрабатываемых

в них информации, предназначенных для автоматизации управления технологическим оборудованием АО «ТАИФ-НК».

Администратор корпоративной информационной системы – работник Общества, ответственный за обеспечение функционирования корпоративной информационной системы АО «ТАИФ-НК».

Администратор АСУ ТП – работник Общества, ответственный за обеспечение функционирование автоматизированной системы управления технологическими процессами АО «ТАИФ-НК».

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Объекты доступа – автоматизированные системы управления техническими процессами, информационные системы, информационные ресурсы и сетевые узлы АО «ТАИФ-НК».

Объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Пользователь информационной системы/автоматизированной системы – работник АО «ТАИФ-НК» или сторонней организации, которому присвоена пара «регистрационное имя – пароль», позволяющая получить доступ к ресурсам информационных систем/автоматизированных систем АО «ТАИФ-НК».

Программное обеспечение – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ, включающая в себя общесистемное, прикладное и специализированное программное обеспечение.

Ресурс информационной/автоматизированной системы – средства, использующиеся в информационной/автоматизированной системе, привлекаемые для обработки информации (например, информационные, программные, технические).

Сеть «Интернет» – информационно-телекоммуникационная сеть общего доступа, доступ к которой обеспечивается по доменным именам и (или) по сетевым адресам.

Wi-Fi (WLAN) – технология беспроводных локальных сетей, позволяющая электронным устройствам подключаться к сети, в основном используя диапазоны 2,4 ГГц и 5 ГГц.

3 ОБОЗНАЧАНИЯ И СОКРАЩЕНИЯ

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
АСУ ТП	Автоматизированная система управления технологическими процессами
БД	База данных
ДИТ	Департамент информационных технологий
ИБ	Информационная безопасность
ИС	Информационная система
ИАС	Информационно-аналитическая система
КИС	Корпоративная информационная система
КИИ	Критическая информационная инфраструктура
МНИ	Машинный носитель информации
Общество	АО «ТАИФ-НК»
ОД	Объект доступа
ОКИИ	Объект критической информационной инфраструктуры
ОИБ УЭБОиР	Отдел информационной безопасности управления по экономической безопасности, охране и режиму

ОИТ и АСУП	Отдел информационных технологий и автоматизации систем управления производством
ОНСИРУРSAP	Отдел нормативно справочной информации, разработок и управления решениями SAP
ПО	Программное обеспечение
УЭБОиР	Управления по экономической безопасности, охране и режиму

4 ОБЩИЕ ПОЛОЖЕНИЯ

4.1. Требования настоящего Положения являются основополагающими при проектировании, создании, введении в действие и эксплуатации информационных и автоматизированных систем и их подсистем.

4.2. Доступ пользователя к компонентам информационной инфраструктуры разрешен только после ознакомления с настоящим Положением под подпись.

4.3. Все документы, программные продукты, созданные, переданные и полученные пользователем во время исполнения своих должностных обязанностей, связанных с работой в информационных и автоматизированных системах, являются и остаются собственностью АО «ТАИФ-НК» и не могут быть личной собственностью ни одного из работников.

4.4. Основными целями обеспечения информационной безопасности в Обществе и настоящего Положения являются:

–обеспечение необходимой доступности ресурсов информационных и автоматизированных систем;

–обеспечение целостности ресурсов информационных и автоматизированных систем;

–обеспечение конфиденциальности информации для обеспечения непрерывности бизнес-процессов, составляющих основу деятельности Общества;

–предупреждение возможности реализации угроз информационным активам Общества.

5 ОРГАНИЗАЦИЯ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА

5.1. Каждый работник АО «ТАИФ-НК», в функциональные обязанности которого входит работа на АРМ, получает его в свое распоряжение в соответствии с заявкой на подключение пользователя к корпоративной информационной системе (*Приложение 1, раздел 1-3,6,7*) с установленным и настроенным ПО. Перечень стандартного ПО, устанавливаемого на АРМ, указан в *Приложении 2*. Заявка направляется от руководителя подразделения пользователя на имя начальника ОИТ и АСУП при согласовании с начальником ОИБ УЭБОиР.

5.2. Заявка на подключение пользователя к корпоративной информационной системе оформляется посредством системы электронного документооборота (СЭД) «ДЕЛО», с заполнением соответствующих разделов. Допускается оформление одной заявки для получения АРМ и требуемых объектов доступа.

5.3. Установка дополнительного ПО (при наличии лицензий на запрашиваемое ПО) производится по заявке (*Приложение 1, раздел 1-4,5.5*) от руководителя подразделения пользователя на имя начальника ОИТ и АСУП при согласовании с начальником ОИБ УЭБОиР и обосновывается необходимостью использования требуемого ПО.

5.4. Изменение аппаратной и программной конфигурации АРМ пользователя проводится специалистами подразделений АО «ТАИФ-НК», отвечающих за обслуживание данного АРМ.

5.5. Устройства ввода-вывода информации (CD/DVD приводы, USB порты, устройства для чтения/записи карт памяти и т.п.) АРМ пользователя должны быть отключены (удалены). При невозможности (нецелесообразности) физического отключения устройств и портов ввода-вывода, они пломбируются согласно п. 9 настоящего Положения или

блокируются при помощи иных средств. Ввод-вывод информации в/из информационной системы в подразделениях организуется через его руководителя (с использованием сетевого ресурса подразделения). Устройства ввода-вывода информации АРМ руководителя подразделения не отключаются (не удаляются) и не пломбируются.

5.6. При обработке на АРМ конфиденциальной информации, размещение и установка технических средств должна исключать возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющим к ней отношения.

6 АНТИВИРУСНАЯ ЗАЩИТА

6.1. Деятельность Общества по антивирусной защите обеспечивает:

−снижение вероятности внедрения вредоносного ПО в информационную инфраструктуру Общества;

−обнаружение и нейтрализацию вредоносного ПО, а также сетевых атак, направленных на информационную инфраструктуру Общества;

−непрерывную защиту Общества от вредоносного ПО, а также сетевых атак, направленных на информационную инфраструктуру Общества.

6.2. К основным внешним признакам заражения вредоносным ПО относят:

−прекращение работы или некорректная работа ранее успешно функционировавших программ и служб;

−вывод на экран непредусмотренных сообщений или изображений;

−подача непредусмотренных звуковых сигналов;

−частые зависания и сбои в работе АРМ.

6.3. В случае обнаружения работниками Общества одного или нескольких из внешних признаков заражения вредоносным ПО, работники Общества уведомляют работника ДИТ о возможном заражении компонента информационной инфраструктуры вредоносным ПО.

6.4. Работники ДИТ проводят мероприятия по определению и устранению причин вышеперечисленных проблем и, в случае подтверждения факта заражения компонента информационной инфраструктуры вредоносным ПО, уведомляют начальника ОИБ УЭБОиР о возможном компьютерном инциденте.

6.5. Работники Общества при получении вложений в сообщениях электронной почты, подключении машинных носителей информации обязаны проверить содержимое файлов, папок, архивных вложений т.д., представляющие угрозу, из контекстного меню антивирусной защиты (предварительно сохранив вложение на диск АРМ) выбрать объект проверки правой клавишей компьютерной мыши, в раскрывающемся списке выбрать – «Проверить на вирусы», при подключении машинного носителя информации – дождаться окончании автоматической проверки).

6.6. Обновление антивирусных баз и модулей приложения системы антивирусной защиты АРМ происходит автоматически, но требует периодической перезагрузки АРМ. Работники Общества обязаны перезагружать АРМ не менее 1 раза в неделю, за исключением АРМ задействованных в непрерывном производственном/технологическом процессе.

6.7. Порядок проведения мероприятий по антивирусной защите информационной инфраструктуры Общества и распределения функциональных обязанностей между работниками подразделений Общества, ответственными за обеспечение антивирусной защиты Общества, описан в регламенте УЭБОиР-Р-07 «Регламент антивирусной защиты объектов КИИ АО «ТАИФ-НК».

7 ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

7.1. Организация парольной защиты направлена на предотвращение и минимизацию ущерба от угроз получения несанкционированного доступа к информационным и автоматизированным системам Общества и несение персональной ответственности пользователей за совершенные в информационной инфраструктуре действия.

7.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех корпоративных ИС АО «ТАИФ-НК» возлагается на работников департамента информационных технологий.

7.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в АСУ ТП АО «ТАИФ-НК» возлагается на работников эксплуатирующих АСУ ТП.

7.4. Контроль за действиями исполнителей и обслуживающего персонала информационных и автоматизированных систем при работе с паролями возлагается на работников ОИБ УЭБОиР.

7.5. Определения и требования к паролям.

7.5.1. Первичный пароль − комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи.

Установку первичного пароля производит системный администратор ОИТ и АСУП при создании новой учетной записи.

При создании первичного пароля, системный администратор обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

7.5.2. Основной пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только работнику организации, используемая для подтверждения подлинности владельца учетной записи.

Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

7.5.3. Внутренним пользователям запрещается хранить пароли в виде текстовых файлов на АРМ, записанными на бумагу на рабочих столах и на элементах АРМ (монитор, клавиатура и пр.) или иным способом, доступным для визуального наблюдения третьими лицами.

7.5.4. При использовании паролей необходимо соблюдать следующую парольную политику.

Минимальная длина паролей для:

−непривилегированных учетных записей – 12 символов,

−привилегированных учетных записей – 23 символов,

−системных учетных записей – 25 символов.

Максимальный срок действия паролей для:

−непривилегированных учетных записей – 40 суток,

−привилегированных учетных записей – 40 суток,

−системных учетных записей – 120 суток.

Алфавит:

−мощность (количество различных символов) алфавита – не менее 60;

−алфавит включает в себя английский алфавит с использованием верхнего и нижнего регистра, цифры от 0 до 9 и специальные символы ([A-Z, a-z, 0-9,!@#$%^&]).

В случае смены пароля отличие нового пароля от старого должно быть не менее чем в шести позициях.

Пароли не должны включать в себя сочетания символов, образующие известные слова, общепринятые сокращения, дату/время года/месяц, фамилию или инициалы владельца

учетной записи и его родственников или иную информацию, позволяющую вычислить пароль учетной записи способом подбора по словарю.

Не допускается использование в пароле 2 следующих друг за другом одинаковых символов для увеличения длины пароля до минимально допустимой.

Максимальное количество безуспешных попыток аутентификации – 3.

Время блокировки учетной записи при достижении максимального количества безуспешных попыток аутентификации – 20 минут.

Время блокировки учетной записи при повторном достижении максимального количества безуспешных попыток аутентификации без предварительной успешной аутентификации – 60 минут.

7.6. Вышеуказанные требования к паролям применимы ко всем автоматизированным и информационным системам Общества при наличии технической возможности.

7.7. Владельцы паролей несут персональную ответственность за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

7.8. Пользователь обязан не реже одного раза в месяц производить смену основного пароля, соблюдая требования настоящего документа.

7.9. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно изменить основной пароль и сообщить о подозрениях в ОИТ и АСУП и ОИБ УЭБОиР.

Восстановление забытого основного пароля пользователя осуществляется системным администратором путем изменения (сброса) основного пароля пользователя на основании служебной записки руководителя подразделения на имя начальника ОИТ и АСУП.

Для предотвращения угадывания паролей системный администратор обязан настроить механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

Разблокирование учетной записи пользователя осуществляется автоматически, по истечении 20 минут.

Для экстренного восстановления забытого основного пароля или разблокировании учетной записи допускается устное уведомление пользователем системного администратора ОИТ и АСУП с предъявлением личного пропуска АО «ТАИФ-НК», либо устная заявка руководителя подразделения начальнику ОИТ и АСУП.

7.10. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и технологической необходимости использования имен и паролей работников в их отсутствие, реализуется следующий алгоритм действий:

–руководитель подразделения, через согласование с начальником ОИБ УЭБОиР, направляет в адрес начальника ОИТ и АСУП служебную записку с указанием фамилии отсутствующего работника, срока, причины и данные работника (ФИО, должность), которому требуется предоставить доступ к компьютеру отсутствующего.

–уполномоченный работник ОИТ и АСУП сбрасывает пароль пользователя и устанавливает первичный пароль.

–допущенный пользователь устанавливает новый основной пароль на АРМ пользователя на период его отсутствия.

–при выходе на работу, пользователь АРМ, на котором был установлен новый основной пароль, сообщает в ОИТ и АСУП (или подразделение, отвечающее за обслуживание данного АРМ) о необходимости смены пароля.

Если по истечению срока, указанного в заявке, уведомление ОИТ и АСУП о смене пароля не поступало, учетная запись пользователя блокируется.

7.11. Полная плановая смена паролей пользователей проводится регулярно, раз в месяц.

7.12. При увольнении работника Общества блокирование персонифицированной учетной записи производится в автоматическом режиме на следующий день после последнего рабочего дня работника на основании данных информационных\автоматизированных систем.

7.13. При переводе на новую должность в другое подразделение Общества, после подписания приказа о переводе работника Общества и ввода данных в информационную систему, блокировка текущих прав доступа учетной записи пользователя производится автоматически на основании данных информационных/автоматизированных систем, контроль блокирования текущих прав осуществляется ОИБ УЭБОиР.

7.14. При увольнении работника Общества, ответственного за реализацию и контроль выполнения деятельности по управлению процессами идентификации и аутентификации (Администратор ИС/АСУ ТП, работники ОИБ УЭБОиР), производится удаление системных учетных записей данного работника со всех информационных систем и устройств, к которым предъявляются требования идентификации и аутентификации.

7.15. Полная внеплановая смена паролей всех пользователей производится по письменному обращению начальника УЭБОиР к директору ДИТ.

7.16. Во избежание получения несанкционированного доступа к ресурсам АРМ работника включается блокировка экрана через 15 минут отсутствия работы на данном компьютере, при этом выход из режима хранителя экрана возможен только при аутентификации пользователя. При необходимости отлучиться от рабочего места пользователь обязан принудительно включить блокировку экрана (одновременным нажатием клавиш «Ctrl», «Alt», «Del» и затем «Блокировка», либо сочетанием клавиш «Win»+«L»).

7.17. Парольная защита также предусматривает генерацию и хранение паролей на специальных аппаратных носителях. Требования к длине и содержимому PIN–кода должны соответствовать рекомендациям производителя аппаратного средства.

Выдача пользователю аппаратного средства хранения пароля производится работником ОИТ и АСУП под подпись.

В случае использования аппаратных средств хранения паролей, при уходе в отпуск, отгул и т.п. пользователь передает его начальнику подразделения.

Работники несут ответственность за утерю аппаратного средства хранения паролей.

При увольнении работника аппаратное средство хранения паролей сдается в ОИТ и АСУП в присутствии работника ОИБ УЭБОиР.

7.18. Порядок управления процессами организации идентификации и аутентификации работников Общества, а также представителей сторонних организаций, действующих в информационной инфраструктуре Общества по предварительному соглашению и в интересах Общества, перечень мероприятий по контролю действий пользователей в информационной инфраструктуре, а также ответственность работников Общества за осуществление указанной деятельности, описан в регламенте УЭБОиР-Р-09 «Регламент идентификации и аутентификации АО «ТАИФ-НК».

8 ДОСТУП К РЕСУРСАМ ИНФОРМАЦИОННОЙ СИСТЕМЫ

8.1. Корпоративная информационная система.

8.1.1. Создание (изменение) учетной записи для работника Общества, выполняется на основании заявки (*Приложение 1, раздел 1-3,6,7*) руководителя структурного подразделения пользователя, с обязательным ознакомлением нового пользователя с требованиями настоящего положения, в адрес начальника ОИТ и АСУП, согласованной с начальником ОИБ УЭБОиР.

8.1.2. При формировании заявки необходимо указание контактных сведений (ФИО, подразделение, должность, табельный номер, контактный телефонный номер) пользователя и руководителя пользователя (ФИО, подразделение), обоснование в соответствии с должностной инструкцией.

8.1.3. Создание (изменение) учетной записи для работника сторонней организации инициируется руководителем структурного подразделения Общества, являющимся инициатором привлечения представителя подрядчика при возникновении необходимости предоставления доступа представителю подрядчика к ресурсам корпоративной информационной системы, АСУ ТП в рамках проведения работ по договору в соответствии с регламентом УЭБОиР-Р-10 «Управления доступом к компонентам информационной инфраструктуры АО «ТАИФ-НК».

8.1.4. При отсутствии указанных выше сведений в заявке или указании сведений, не раскрывающих необходимость создания (изменения) учетной записи, принимается решение об отказе в создании (изменении) учетной записи.

8.2. Электронная почта.

8.2.1. Учетная запись электронной почты пользователя формируется при создании учетной записи для работника Общества (*Приложение 1, раздел 1-3,4.2,6*) и заполнении соответствующего раздела заявки. Заявка направляется от руководителя подразделения пользователя на имя начальника ОИТ и АСУП при согласовании с начальником ОИБ УЭБОиР.

8.2.2. По умолчанию электронная почта создаётся без возможности отправки внешним адресатам (внутренняя).

8.2.3. При указании в разделе 4.2. «внешней» необходимо дополнительно обосновать в пункте 6 заявки.

8.2.4. Система электронной почты АО «ТАИФ-НК» предоставляется работникам в целях выполнения ими своих должностных обязанностей.

8.2.5. С целью поддержания единого делового стиля при общении посредством электронной почты работник обязан создать подпись для электронных сообщений по единой форме, размещенной в блоке ссылок электронной базы документов. Порядок создания и применения подписи для электронных сообщений приведен в *Приложении 3*.

8.2.6. Размер почтового ящика для хранения оперативных почтовых сообщений устанавливается в размере 300МБ. Для хранения большего объема почтовых сообщений, пользователь настраивает в почтовом клиенте автоматическое архивирование в целях разгрузки оперативного хранилища.

8.2.7. Все сообщения, созданные, переданные и полученные с помощью системы электронной почты являются и остаются собственностью АО «ТАИФ-НК». Сообщения не могут быть личной собственностью ни одного из работников.

8.2.8. Служебную переписку разрешается вести только через корпоративный почтовый сервер АО «ТАИФ-НК». Для обеспечения безопасной переписки пользователю необходимо руководствоваться инструкцией по безопасной работе с корпоративной электронной почтой (*Приложение 4*).

8.2.9. Использовать систему электронной почты можно исключительно для выполнения своих должностных обязанностей. Электронная почта не предназначена для применения в личных целях.

8.2.10. Работники отдела ИБ УЭБОиР, имеют право просматривать, контролировать, изымать и использовать все сообщения, созданные, полученные или переданные с помощью системы электронной почты, с целью обеспечения безопасности. Сообщения электронной почты с признаками нанесения ущерба доводятся до сведения Генерального директора и начальника управления по экономической безопасности, охране и режиму АО «ТАИФ-НК» без разрешения работника.

8.2.11. Работник, нарушивший эти правила или использующий систему электронной почты в незаконных либо личных целях, подвергается дисциплинарному наказанию.

8.2.12. Передача конфиденциальной информации по системе электронной почты сторонним организациям и физическим лицам регламентируется разделом «Положения о коммерческой тайне АО «ТАИФ-НК».

8.3. Сеть «Интернет».

8.3.1. Подключение пользователя к ресурсам сети «Интернет» выполняется по заявке руководителя подразделения пользователя (*Приложение 1, раздел 1-3,4.1.,5,6*) и заполнении соответствующего раздела. Заявка направляется от руководителя подразделения пользователя на имя начальника ОИТ и АСУП, при согласовании заместителем генерального директора по направлению деятельности/главным бухгалтером/главным инженером Общества, начальником ОИБ УЭБОиР.

8.3.2. Ресурсы сети «Интернет» используются пользователями только для решения производственных вопросов в соответствии с должностными обязанностями.

8.3.3. ОИБ УЭБОиР на постоянной основе ведет контроль за использованием ресурсов сети «Интернет».

8.3.4. Доступ из сети «Интернет» к ресурсам информационно-вычислительной сети организации осуществляется с использованием защищенного канала при наличии технической возможности установки средств защиты на АРМ мобильного пользователя. Заявка на удаленное подключение с обоснованием такого подключения согласовывается начальником ОИБ УЭБОиР и начальником УЭБОиР (*Приложение 1, раздел 1-4,5.8.,6*).

8.4. Подключение мобильных и стационарных электронных устройств к корпоративным беспроводным сетям (по протоколу IEEE 802.11 «Wi-Fi»).

8.4.1. Доступ к корпоративной сети посредством беспроводного подключения осуществляется при отсутствии возможности проводного подключения.

8.4.2. Подключение пользователя к корпоративной беспроводной сети выполняется по заявке руководителя подразделения пользователя (*Приложение 1, раздел 1-3,4.6.,5,6*) и заполнении соответствующего раздела. Заявка направляется от руководителя подразделения пользователя на имя начальника ОИТ и АСУП при согласовании с начальником ОИБ УЭБОиР.

8.4.3. Временный доступ к корпоративной беспроводной сети для работника сторонней организации инициируется руководителем структурного подразделения Общества, являющимся инициатором привлечения представителя подрядчика при возникновении необходимости, оформляется по заявке (*Приложение 1, раздел 1-4,5.6,6*), как минимум за три рабочих дня до начала доступа в адрес начальника ОИТ и АСУП, согласованную с начальником ОИБ УЭБОиР. В заявке необходимо указать время и сроки проведения мероприятия, название организации, контактный телефон. После оформления заявки для представителя подрядчика активируется временная учетная запись, атрибуты которой отправляются ответственному лицу, подавшему заявку, на его электронный адрес.

8.5. Доступ к базам данных информационных систем.

8.5.1. Доступ к базам данных информационной системы осуществляется на основании заявки руководителя работника (*Приложение 1, раздел 1-3,4.3.,4.4.,5,6*), оформляющего допуск, на имя начальника ОИТ и АСУП, при согласовании соответствующего руководителя и начальника ОИБ УЭБОиР. В заявке на допуск работника к базам данных информационной системы должны быть указаны: ФИО, должность работника, обоснование подключения к базе данных со ссылкой на должностную инструкцию, срок подключения.

8.5.2. Пункт 8.5.1 не относится к подразделениям, формирующим соответствующую базу данных. Подключение работников данных подразделений осуществляется на основании служебной записки руководителя подразделения в адрес директора ДИТ.

8.5.3. Подключение сотрудников сторонних организаций осуществляется согласно п.8.5.1 с дополнением согласования начальником УЭБОиР. В обосновании подключения должна быть указана ссылка на пункты договора со сторонней организацией, требующих необходимость использования данных подключаемой базы. С данной сторонней организацией должно быть заключено соглашение (договор, пункт договора и т.п.) о конфиденциальности. Подключаемый к базе данных работник подписывает обязательство о неразглашении конфиденциальных сведений АО «ТАИФ-НК».

8.5.4. Процессы копирования и хранения баз данных на внешних носителях информации для последующего восстановления системы осуществляется на основании утвержденного регламента «Резервного копирования данных ИТ-инфраструктуры АО «ТАИФ-НК» работниками департамента информационных технологий.

8.6. Доступ к автоматизированным системам управления производством.

8.6.1. Подключение пользователя к системе электронного документооборота (СЭД) «Дело», системе программ «1С:Предприятие» выполняется на основании заявки руководителя работника (*Приложение 1, раздел 1-3,4.3.,4.4.,5,6*), на имя заместителя директора по НСИРУРSAP, при согласовании соответствующего руководителя и начальника ОИБ УЭБОиР.

8.6.2. Подключение пользователей к автоматизированной системе управления производством PI System осуществляется согласно «Регламента № ОИТ и АСУП-Р-01-12 взаимодействия подразделений АО «ТАИФ-НК» при работе с автоматизированной системой управления производством PI System».

8.6.3. Доступ пользователей к автоматизированной системе управления производством SAP ERP предоставляется согласно «Регламента регистрации и ведения пользователей в системе SAP ERP».

8.7. Доступ к системам обеспечения информационной безопасности.

Доступ работников ОИБ УЭБОиР к системам обеспечения информационной безопасности осуществляется на основании служебной записки начальника ОИБ УЭБОиР в адрес начальника УЭБОиР.

8.8. Использование сетевых ресурсов.

Во избежание утери информации (случайное удаление, временная неисправность АРМ) работникам рекомендуется критически важную информацию хранить на общедоступных сетевых ресурсах АО «ТАИФ-НК».

9 ОПЕЧАТЫВАНИЕ СИСТЕМНЫХ БЛОКОВ, ДИСКОВОДОВ, USB-ПОРТОВ АРМ

9.1. Опечатывание системных блоков, дисководов, USB-портов АРМ производится работниками ОИБ УЭБОиР и ОИТ и АСУП. Опечатывание производится только при невозможности блокировки указанных устройств программными средствами.

9.2. Ввод в эксплуатацию новых АРМ производится только после опечатывания системных блоков и USB-портов. Дисководы и CD-приводы новых АРМ отключаются отделом ИТ и АСУП на аппаратном уровне. В случае контроля доступа к устройствам ввода/вывода программными средствами, опечатывание системных блоков, USB-портов, дисководов и CD-приводов устройства не производится.

9.3. После опечатывания ставится отметка в таблице Журнала опечатывания (*Приложение 5*), пользователь АРМ должен убедиться в установке и целостности пломб.

9.4. Ежедневно, до включения АРМ, пользователь обязан проверить целостность установленных пломб. При наличии нарушения целостности – незамедлительно сообщить в ОИБ УЭБОиР.

9.5. В период длительного отсутствия (отпуск, командировка, больничный и т.д.) пользователя АРМ ответственным за проверку целостности установленных пломб является руководитель подразделения.

9.6. Установление факта нарушения целостности пломб производится работниками ОИБ УЭБОиР с привлечением работников ОИТ и АСУП и работника подразделения пользователя. Работниками ОИБ УЭБОиР, ОИТ и АСУП проверяется целостность данных на жестком диске, аппаратных и программных средств АРМ, а также устанавливаются причины нарушения целостности пломб.

9.7. Перед началом профилактических/ремонтных работ на АРМ в подразделениях работник ОИТ и АСУП проверяет целостность пломб и при наличии нарушения – незамедлительно сообщает в ОИБ УЭБОиР. По завершении работ производится повторное опечатывание с отметкой в таблице журнала опечатывания.

9.8. Ввод/вывод информации из информационной системы на внешние носители производится только через АРМ руководителя подразделения.

9.9. В исключительных случаях допускается применение портов ввода-вывода на АРМ пользователя по заявке руководителя подразделения в адрес ОИТ и АСУП, согласованной с начальником ОИБ УЭБОиР (*Приложение 1, раздел 1-3,4.7.,5,6*).

10 УПРАВЛЕНИЕ МАШИННЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ

10.1. Деятельность Общества по управлению МНИ направлена на предотвращение и минимизацию ущерба от угроз получения несанкционированного доступа к локальной вычислительной сети Общества, распространения вредоносного программного обеспечения, а также угроз, связанных с утечкой или разглашением защищаемой информации.

10.2. В Обществе используются МНИ следующего типа:

−съемные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

−носители информации, встроенные в корпус АРМ, электронного устройства (накопители на жестких дисках).

10.3. В Обществе допускается использование МНИ выданных Обществом, также личных, проверенных средствами антивирусного ПО, учтенных в «Журнале учета машинных носителей информации» (Приложение 1. УЭБОиР-Р-08 «Регламент управления машинными носителями информации АО «ТАИФ-НК»).

10.4. МНИ Общества, выдаются исключительно для выполнения работниками своих должностных обязанностей, согласно должностной инструкции.

10.5. При использовании МНИ за пределами контролируемой зоны Общества работник обязан обеспечить меры защиты, направленные на предотвращение несанкционированного доступа к ним, их хищения или утрате, а также исключить заражение вредоносным ПО.

10.6. Работники Общества в полной мере участвуют в процессе обеспечения информационной безопасности как используемых, так и неиспользуемых МНИ в рамках своих должностных обязанностей.

10.7. Работники Общества несут ответственность за соблюдение конфиденциальности и обеспечение целостности информации, хранящейся на МНИ, пользователями которых они являются.

10.8. Использование МНИ, в том числе обеспечение информационной безопасности при их эксплуатации в Обществе, их защиты в процессе использования в информационной инфраструктуре Общества, а также ответственность работников Общества за осуществление указанной деятельности, описаны в регламенте УЭБОиР-Р-08 «Регламент управления машинными носителями информации АО «ТАИФ-НК».

11 ЗАЩИТА ТЕХНИЧЕСКИХ СРЕДСТВ И СИСТЕМ ОБЪЕКТОВ КИИ

11.1 Защищаемыми помещениями в АО «ТАИФ-НК» являются:

−серверные, аппаратные, контроллерные помещения;

−помещения учрежденческо-производственной АТС;

−иные помещения, обозначенные как помещения с ограниченным доступом.

11.2 Защищаемые помещения должны быть оборудованы надежными автоматическими замками с контролем доступа, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов.

11.3 Доступ в защищаемые помещения предоставляется на основании служебной записки, направленной в адрес начальника отдела охраны и режима УЭБОиР, после согласования с начальником ОИБ УЭБОиР. Работниками отдела охраны и режима УЭБОиР вносятся изменения в систему контроля удаленного доступа. Копии согласованных служебных записок с перечнем работников, допущенных к защищаемым помещениям, передаётся и хранится у сотрудника охраны (дежурного), передаются на соответствующие КПП работникам ООО «ЧОП Кеннард-НК» для осуществления контроля по выдаче ключей от защищаемых помещений.

11.4 Выполнение уборки, либо работы представителями сторонних организаций в защищаемых помещениях должны производиться в присутствии ответственного, за которым закреплены данные технические средства, или дежурного по подразделению с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

11.5 Выполнение уборки, либо работы представителями сторонних организаций в кабинетах руководителей АО «ТАИФ-НК» должны производиться в присутствии охраны и (или) ответственного за исполнение данных работ.

11.6 Порядок организации защиты технических средств и систем, в том числе правила и процедуры их эксплуатации в Обществе, исключающие возможности несанкционированного доступа к конфиденциальной информации, а также ответственность работников Общества за осуществление указанной деятельности, описан в регламенте УЭБОиР-Р-15 «Регламент защиты технических средств и систем объектов КИИ АО «ТАИФ-НК».

12 ОГРАНИЧЕНИЯ ПРИ РАБОТЕ НА ПЭВМ

Пользователю АРМ запрещается:

12.1 Несогласованный доступ, а также доступ без ознакомления с настоящим Положением к любым информационным, автоматизированным системам и компонентам информационной системы АО «ТАИФ-НК».

12.2 Осуществлять изменение аппаратно-программной конфигурации АРМ, настройки операционной системы, ПО и средств защиты.

12.3 Снятие пломб контроля вскрытия АРМ.

12.4 Изменение доменных прав на иные, кроме как установленные при создании учетной записи.

12.5 Сообщать логин и пароль другим лицам, в том числе работникам ДИТ и УЭБОиР, записывать их, а также пересылать открытым текстом в электронных сообщениях.

12.6 Передавать аппаратные средства хранения паролей и ключей иным лицам, кроме руководителя подразделения.

12.7 Использовать программные средства доступа в Интернет с правами администратора.

12.8 Принимать посетителей во время обработки конфиденциальной информации.

12.9 Передавать конфиденциальную информацию, в том числе относящуюся к коммерческой тайне, через общедоступные каталоги, сети общего пользования, внешние носители информации, сеть «Интернет» и электронную почту в открытом (незашифрованном) виде и без заключения соглашения (договор, пункт договора и т.п.) о конфиденциальности.

12.10 Проносить на объекты АО «ТАИФ-НК», ПАО «Нижнекамскнефтехим»: видеозаписывающую аппаратуру, фотоаппараты, телефоны с встроенной камерой, магнитные и оптические носители информации без согласования со службой безопасности ПАО «Нижнекамскнефтехим» и УЭБОиР АО «ТАИФ-НК». Пронос указанной техники на территорию АО «ТАИФ-НК» за пределами ПАО «Нижнекамскнефтехим» должен быть согласован с УЭБОиР АО «ТАИФ-НК».

12.11 Несогласованная руководителем подразделения работника передача документов и продуктов деятельности работника за пределы корпоративной информационной системы АО «ТАИФ-НК» любым способом и на любых носителях.

12.12 Несогласованное с ОИТ и АСУП и ОИБ УЭБОиР использование иных средств электронного документооборота и общедоступных ресурсов передачи данных, в том числе ресурсов сети «Интернет», кроме принятых в АО «ТАИФ-НК».

12.13 Использование ресурсов АО «ТАИФ-НК» (в том числе сеть «Интернет», электронная почта, офисная техника) для личных целей.

12.14 Использование системы электронной почты для агитации или рекламы коммерческих предприятий, пропаганды религиозных или политических идей, оскорбительных или провокационных сообщений и для других целей, не связанных с выполнением должностных обязанностей.

12.15 Использование системы электронной почты и сети «Интернет» для передачи (выгрузки) или получения (загрузки) материалов, защищенных авторским правом, торговых секретов, внутренней финансовой информации или аналогичных документов лицами, не имеющими соответствующих полномочий.

12.16 Предоставлять работникам сторонних организаций ресурсы информационных и автоматизированных систем АО «ТАИФ-НК» без оформленного Соглашения о конфиденциальности, либо условий, указанных в договоре о предоставлении ресурсов.

13 КОНТРОЛЬ И ОТВЕТСТВЕННОСТЬ

13.1 Контроль за выполнением требований настоящего Положения возлагается на начальника ОИБ УЭБОиР.

13.2 Руководители подразделений несут ответственность за исполнение подчиненными работниками требований настоящего Положения.

13.3 Пользователи несут персональную ответственность за нарушения требований настоящего Положения.

13.4 Нарушение требований обеспечения информационной безопасности Общества является чрезвычайным происшествием. По всем фактам проводится служебная проверка комиссией, инициируемой начальником ОИБ УЭБОиР.

13.5 Основанием для проведения служебной проверки являются сведения о возможном нарушении работниками АО «ТАИФ-НК» требований информационной безопасности и защиты информации конфиденциального характера, или установленный факт утечки информации.

13.6 Работники, проводящие служебную проверку, в целях решения задач, имеют право:

–на беспрепятственный допуск в здания и помещения, ко всем АРМ и локальным ресурсам, необходимым для проведения служебной проверки;

–на ознакомление со служебной документацией подразделения, в том числе ограниченного доступа, имеющей прямое или косвенное отношение к проводимой проверке;

–истребовать копии документов, объяснительных записок в проверяемом подразделении для приобщения их к материалам служебной проверки. По требованию работника ОИБ УЭБОиР, проводящего служебную проверку, руководитель подразделения обязан предоставить копию требуемого служебного документа для его приобщения к материалам служебной проверки.

–привлекать к проведению служебной проверки, по согласованию с руководителями подразделений, работников Общества, обладающих необходимыми специальными познаниями;

–по необходимости вызывать работников Общества, поставив в известность и согласовав с руководством, и получать от них объяснения и иную информацию, запрашивать и получать необходимые сведения, разъяснения и консультации в подразделениях Общества и, при необходимости, иных организациях.

При необходимости, запросы в подразделения направляются в письменном виде за подписью начальника УЭБОиР, и должны исполняться работниками незамедлительно после их получения.

13.7 За нарушение требований настоящего Положения работники и их руководители несут ответственность и к ним могут быть применены меры дисциплинарного наказания.

Начальник УЭБОиР С.М. Малов