Общество с ограниченной ответственностью

ГАЗПРОМ
ДОБЫЧА
ОРЕНБУРГ

СТАНДАРТ ОРГАНИЗАЦИИ

ПОЛИТИКА
информационной безопасности автоматизированной системы управления технологическими процессами в ООО «Газпром добыча Оренбург»

СТО 25 - 04 - 2016

г. Оренбург

П р е д и с л о в и е

1. РАЗРАБОТАН	Службой корпоративной защиты ООО «Газпром добыча Оренбург»
2. ВНЕСЕН	Службой корпоративной защиты ООО «Газпром добыча Оренбург»
3. УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ	приказом генерального директора ООО «Газпром добыча Оренбург» **от 09.11.2016 № 373**
4. ВВЕДЕН ВПЕРВЫЕ/ВЗАМЕН	Взамен СТО 25-03-2010 «Политика информационной безопасности автоматизированной системы управления технологическими процессами в ООО «Газпром добыча оренубрг», утвержденного приказом генерального директора ООО «Газпром добыча Оренбург» от 27.09.2010 № 285 (впервые или сведения о документе, взамен которого введен данный стандарт) с **21.11.2016** года (дата введения стандарта в действие)
5. ЛИСТОВ	26 (общее количество листов в документе)

Содержание

Введение

Настоящий стандарт разработан в целях совершенствования комплексной системы защиты информации ООО «Газпром добыча Оренбург» (далее – Общество) и устанавливает единый подход при разработке и реализации мер обеспечения информационной безопасности во всех структурных подразделениях Общества.

Стандарт разработан авторским коллективом под руководством Алпеева И.В. на основе Рекомендаций ПАО «Газпром» Р Газпром 4.2-0-003-2009 «Типовая политика информационной безопасности автоматизированной системы управления технологическими процессами».

1. Область применения и назначения

Настоящий стандарт определяет основные принципы политики информационной безопасности Общества и предназначен для применения структурными подразделениями администрации, подразделениями, созданными при администрации, и обособленными структурными подразделениями Общества.

2. Нормативные ссылки

В настоящей Политике использованы следующие документы:

СТО Газпром 4.2-0-001-2009	Система обеспечения информационной безопасности ОАО «Газпром». Документы системы.
СТО Газпром 4.2-0-004-2009	Система обеспечения информационной безопасности ОАО «Газпром». Базовая модель информационной безопасности корпоративных информационно-управляющих систем.
СТО Газпром 4.2-1-001-2009	Система обеспечения информационной безопасности ОАО «Газпром». Основные термины и определения.
СТО Газпром 4.2-2-002-2009	Система обеспечения информационной безопасности ОАО «Газпром». Требования к автоматизированным системам управления технологическими процессами.
СТО Газпром 4.2-3-001-2009	Система обеспечения информационной безопасности ОАО «Газпром». Руководство по разработке требований к объектам защиты.
СТО Газпром 4.2-3-003-2009	Система обеспечения информационной безопасности ОАО «Газпром». Анализ и оценка рисков.
СТО Газпром 4.2-3-004-2009	Система обеспечения информационной безопасности ОАО «Газпром». Классификация объектов защиты.

3. Термины, определения и сокращения

В настоящей Политике применены термины в соответствии с СТО Газпром 4.2-1-001 и следующие сокращения:

АРМ	автоматизированное рабочее место;
АСУ ТП	автоматизированная система управления технологическими процессами;
ИБ	информационная безопасность;
ИУС ПХД	информационно-управляющая система производственно-хозяйственной деятельности;
ЛВС	локальная вычислительная сеть;
ОС	операционная система;
ПО	программное обеспечение;
СВ	средства виртуализации;
СТД	средства терминального доступа;
ТЗ	техническое задание.

4. Общие положения

Настоящая Политика ИБ разработана с учетом требований федерального законодательства, требований нормативных и организационно-распорядительных документов ПАО «Газпром» по вопросам обеспечения ИБ, в том числе политики ИБ ПАО «Газпром» [1], а также Политики ИБ Общества [2].

Настоящая Политика ИБ выражает позицию руководства в отношении обеспечения ИБ АСУ ТП и является методологической основой для разработки нормативных и организационно-распорядительных документов Общества в области обеспечения ИБ АСУ ТП.

Исполнение положений настоящей Политики ИБ является обязательным для всех пользователей АСУ ТП.

Под АСУ ТП в настоящем стандарте понимается система, состоящая из персонала и комплекса средств автоматизации его деятельности и формирующая управляющее воздействие на технологические процессы.

Комплекс средств автоматизации включает в себя:

– системы диспетчерского управления (АРМ пользователей и серверы, на которых установлено системное и прикладное ПО, а также набор сетевого оборудования для организации ЛВС и средств ее защиты (средства межсетевого экранирования, средства обнаружения и предотвращения вторжений);

– системы локальной автоматики (системы автоматического управления, концентраторы, контроллеры, пункты управления технологическими объектами);

– устройства сопряжения с объектами (оборудование датчиков и программируемые логические контроллеры).

5. Принципы и направления обеспечения информационной безопасности в автоматизированной системе управления технологическими процессами

Целью обеспечения ИБ АСУ ТП является повышение уровня устойчивости ее функционирования, стабильности исполнения реализуемых технологических процессов путем предотвращения и (или) снижения возможного ущерба от несанкционированных воздействий на объекты защиты АСУ ТП.

Обеспечение ИБ в АСУ ТП основывается на следующих принципах:

– обязательной идентификации и классификации объектов защиты в соответствии с СТО Газпром 4.2-3-004;

– учета при выборе мер и средств защиты частной модели угроз, построенной в соответствии с СТО Газпром 4.2-0-004;

– оценки рисков реализации угроз ИБ в соответствии с СТО Газпром 4.2-3-003;

– регламентации порядка доступа к объектам защиты.

Объектами защиты в АСУ ТП являются:

– серверное оборудование (сервер системы SCADA, архивные, коммуникационные и другие серверы);

– системы локальной автоматики (системы автоматического управления, концентраторы, контроллеры, пункты управления технологическими объектами);

– устройства сопряжения с объектами (оборудование датчиков и программируемые логические контроллеры);

– АРМ операторов и специалистов;

– сетевое оборудование (коммутаторы, маршрутизаторы, фронтальные процессоры, интегрирующие контроллеры, контроллеры связи с объектами);

– каналы передачи данных;

– ПО;

– технологическая информация (в том числе сигналы, команды управления, данные о параметрах (состоянии) управляемого технологического объекта (процесса).

В состав АСУ ТП входит система диспетчерского управления, которая строится как ЛВС, изолируемая за счет средств фильтрации информационных потоков от внешних по отношению к ней сетей, в том числе ЛВС ИУС ПХД Общества. Информационное взаимодействие с ИУС ПХД заключается в передаче технологической информации из АСУ ТП в ИУС ПХД и получении из ИУС ПХД необходимой информации, связанной с управлением АСУ ТП и обновлением ПО и конфигураций элементов АСУ ТП и входящих в ее состав средств защиты.

Основными угрозами ИБ в АСУ ТП являются:

– несанкционированное вмешательство в управление технологическими процессами;

– нарушение функционирования АСУ ТП или отдельных ее элементов;

– несанкционированный доступ к информации, хранимой в базах данных АСУ ТП и передаваемой по каналам передачи данных.

В результате реализации угроз ИБ могут быть нарушены:

– целостность (утрата, уничтожение, модификация) информации;

– доступность (блокирование) информации и отдельных элементов АСУ ТП;

– конфиденциальность (утечка, перехват, съем, копирование, хищение, разглашение) информации.

Обеспечение ИБ АСУ ТП осуществляется по следующим направлениям, реализуемым организационно-техническими мерами защиты.

Физическая защита, включая:

– защиту технических средств обработки, хранения и передачи информации;

– защиту зданий, сооружений и помещений.

Обеспечение ИБ при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов, включая:

– организацию безопасной эксплуатации средств обработки, хранения и передачи информации;

– защиту от вредоносного ПО;

– резервирование серверов, сетевого оборудования, средств защиты и каналов передачи данных;

– обеспечение безопасности сетевой инфраструктуры;

– защиту программного обеспечения;

– регистрацию и учет событий ИБ;

– контроль защищенности;

– криптографическую защиту.

Контроль доступа, в том числе:

- управление доступом пользователей;
- определение ответственности пользователей;
- контроль доступа к прикладным системам;
- контроль доступа к ОС;
- контроль сетевого доступа;
- обеспечение безопасности при использовании мобильных устройств;
- обеспечение безопасности в беспроводных сетях;
- контроль доступа к сетевому оборудованию.

Реализация организационно-технических мер обеспечения ИБ в АСУ ТП достигается в первую очередь путем:

- наделения пользователей АСУ ТП правами доступа и привилегиями по работе в АСУ ТП;
- корректного использования и администрирования встроенных механизмов безопасности технических средств обработки, хранения и передачи информации и наложенных средств защиты, входящих в состав АСУ ТП;
- контроля функционирования и настроек механизмов безопасности, а также соблюдения требований по ИБ;
- физической защиты технических средств обработки, хранения и передачи информации от неправомерного доступа к ним.

Функции администрирования выполняются специалистами подразделений, отвечающих за эксплуатацию объектов защиты (системными и сетевыми администраторами, а также администраторами прикладных систем и администраторами ИБ), а функции контроля – сотрудниками отдела ИБ СКЗ.

Обязанности пользователей АСУ ТП по обеспечению ИБ зависят от занимаемой должности и определены нормативными и организационно-распорядительными документами Общества в области ИБ.

6. Порядок обеспечения информационной безопасности на этапах жизненного цикла автоматизированной системы управления технологическими процессами

Информационная безопасность АСУ ТП обеспечивается на всех этапах ее жизненного цикла с учетом роли всех вовлеченных в этот процесс сторон

(разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих организаций и надзорных органов).

Отдел ИБ СКЗ непосредственно участвует во всех этапах жизненного цикла АСУ ТП по части вопросов ИБ.

Жизненный цикл АСУ ТП включает в себя следующие этапы:

- обоснование требований к системе;
- разработка (модернизация) системы;
- ввод системы в действие;
- эксплуатация системы;
- вывод системы из эксплуатации.

6.1. Этапы обоснования требований и разработки (модернизации)

Порядок разработки требований по ИБ, предъявляемых к АСУ ТП, регламентируется СТО Газпром 4.2-3-001.

Ответственность за включение в ТЗ на создание (модернизацию) АСУ ТП, а также в техническую, программную, конструкторскую, проектную и эксплуатационную документацию обоснованных требований по защите обрабатываемой информации и контроль их выполнения в процессе экспертизы документации, испытаний и приемки разрабатываемых проектов согласно п. 5.2.2 СТО Газпром 4.2-3-001 возлагается на структурное подразделение Общества, в интересах которого осуществляется разработка (модернизация) АС.

ТЗ в части требований по обеспечению ИБ в АСУ ТП согласовывается со Службой корпоративной защиты ПАО «Газпром».

Требования по ИБ формируются с учетом экономической целесообразности, уровней критичности объектов защиты, режима работы АСУ ТП и не должны быть ниже требований, установленных в СТО Газпром 4.2-2-002.

Этап разработки (модернизации) АСУ ТП завершается оценкой ее соответствия требованиям ИБ (сертификацией) в Системе добровольной сертификации ГАЗПРОМСЕРТ.

6.2. Этап ввода в эксплуатацию

Обеспечение ИБ АСУ ТП на этапе ввода в эксплуатацию осуществляется организацией, ответственной за ввод в эксплуатацию. Подразделение ИБ осуществляет контроль соблюдения мер ИБ при вводе в эксплуатацию.

Перед вводом АСУ ТП в эксплуатацию в целевой среде осуществляется запуск системы в тестовом режиме в выделенной тестовой среде.

Процедуры установки и запуска АСУ ТП должны обеспечивать безопасный запуск системы в тестовом режиме, а также перенос в целевую среду и переход из тестового режима в режим эксплуатации.

Предпринимаются меры по контролю правильности поставляемой версии программного обеспечения, настройке всех необходимых параметров функций безопасности и проверке их работоспособности, смене настроек по умолчанию и запуску системы безопасным способом в соответствии с рекомендациями разработчика.

6.3. Этап эксплуатации

В процессе эксплуатации АСУ ТП обеспечение ИБ достигается:

– периодическим проведением переоценки рисков для принятия необходимых мер ИБ;

– планированием и выполнением процедур минимизации ущерба и восстановления АСУ ТП, расследованием причин нарушений ИБ и принятием мер по исключению подобных случаев.

Принимаются меры по недопущению внесения в АСУ ТП изменений, приводящих к нарушению ее функциональности или появлению недокументированных возможностей. Выполняется регистрация всех событий, которые могут иметь отношение к ИБ, мониторинг работы технических средств и выполнение организационных мер ИБ, обеспечивается обратная связь для корректирующих действий после внесения изменений в АСУ ТП.

Эксплуатация средств и систем защиты АСУ ТП должна сопровождаться организацией-разработчиком весь срок их службы.

В процессе сопровождения подразделением ИБ рассматриваются и анализируются все предлагаемые или сделанные изменения в конфигурации АСУ ТП, включая изменения политик, правил и процедур. При значительном изменении уровня остаточных рисков, проводится повторная оценка соответствия АСУ ТП требованиям ИБ.

6.4. Этап вывода из эксплуатации

На стадии вывода из эксплуатации отдельных элементов АСУ ТП должно быть обеспечено архивирование, перемещение и гарантированное (по возможности) удаление информации из запоминающих устройств.

7. Физическая защита

7.1. Защита технических средств обработки, хранения и передачи информации

В целях предотвращения несанкционированного доступа к информации и ее утечки, хищения технических средств обработки и хранения информации и несанкционированного управления ими, а также простоев в функционировании АСУ ТП обеспечивается физическая защита входящих в нее технических средств.

Физическая защита технических средств осуществляется в соответствии с требованиями СТО Газпром 4.2-2-002.

Серверное оборудование и критичное сетевое оборудование размещаются в запираемых шкафах с сигнализацией, располагаемых в специализированных помещениях (серверных), ограничивающих доступ к ним посторонних лиц.

Перед утилизацией или передачей в ремонт технических средств выполняется гарантированное удаление информации с них.

Кабельные сети прокладываются так, чтобы максимально ограничить несанкционированный доступ к ним.

7.2. Защита зданий, сооружений и помещений

В целях обеспечения безопасности технических средств АСУ ТП осуществляется защита зданий, сооружений и помещений АСУ ТП.

Защита зданий, сооружений и помещений осуществляется в соответствии с требованиями СТО Газпром 4.2-2-002.

Здания и сооружения, в которых размещаются технические средства АСУ ТП, обеспечиваются инженерно-техническими средствами охраны и средствами антитеррористической защиты.

Помещения, в которых размещаются критически важные технические средства АСУ ТП, оборудуются средствами пожарной безопасности, вентиляции и кондиционирования. Доступ в такие помещения разрешается работникам Общества

только для выполнения должностных обязанностей по обслуживанию технических средств АСУ ТП. Доступ в помещения ограничивается средствами контроля и управления доступом.

При выполнении работ в помещениях, где размещаются критически важные технические средства АСУ ТП, лицами, чья деятельность не связана непосредственно с их обслуживанием, обеспечивается контроль их деятельности.

8. Обеспечение информационной безопасности при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов

8.1. Организация безопасной эксплуатации средств обработки, хранения и передачи информации

Правила безопасного использования прикладных систем и средств вычислительной техники, безопасной эксплуатации сетевой инфраструктуры АСУ ТП определяются нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области ИБ.

Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации разделяются и возлагаются на специально выделенных для этого работников.

Изменения в конфигурации средств обработки и хранения информации, а также изменения в сетевой инфраструктуре, конфигурации сетевого оборудования выполняются системными и сетевыми администраторами. Изменения в конфигурации средств защиты выполняются администраторами ИБ. Все изменения регистрируются в соответствующих журналах.

Самостоятельное изменение конфигурации средств обработки, хранения и передачи информации пользователями АСУ ТП запрещено.

Использование съемных носителей информации в АСУ ТП запрещено.

При размещении средств разработки, тестирования и эксплуатации обеспечивается их физическое или логическое разделение в целях снижения риска несанкционированного доступа или внесения изменений в систему.

8.2. Защита от вредоносного программного обеспечения

В целях предотвращения проникновения, обнаружения внедрения и нейтрализации вредоносного ПО в АСУ ТП применяются средства защиты от вредоносного ПО.

Средства защиты от вредоносного ПО устанавливаются на серверном оборудовании и АРМ операторов и специалистов АСУ ТП. В случае технической невозможности установки средств защиты от вредоносного ПО на конкретных серверах и АРМ, принимаются дополнительные организационные и технические меры защиты. Дополнительные меры защиты определяются подразделением ИБ на основе анализа рисков с учетом особенностей режимов функционирования АСУ ТП.

Управление и обновление средств защиты от вредоносного ПО осуществляется централизованно.

Разрешается использование только сертифицированных на соответствие требованиям безопасности информации средств защиты от вредоносного ПО.

Администрирование средств защиты от вредоносного ПО осуществляется системным администратором. Настройки системы защиты от вредоносного ПО согласовываются и контролируются администратором ИБ. Пользователи АСУ ТП несут ответственность за соблюдение установленных в Обществе правил защиты от вредоносного ПО.

Случаи проникновения и внедрения вредоносного ПО расследуются в рамках мероприятий по управлению инцидентами ИБ. Восстановление систем после воздействия вредоносного ПО осуществляется в рамках мероприятий по обеспечению непрерывности бизнес-процессов.

8.3. Резервирование серверов, сетевого оборудования и каналов передачи данных автоматизированной системы управления технологическими процессами

В целях обеспечения бесперебойного функционирования АСУ ТП осуществляется резервирование критически важных серверов и АРМ операторов, сетевого оборудования, средств защиты и каналов передачи данных.

Перечень критически важных средств защиты, обработки, хранения и передачи информации формируется в результате проведения идентификации и классификации объектов защиты АСУ ТП, проводимых в соответствии с СТО Газпром 4.2-3-004.

В целях резервирования серверов и АРМ осуществляется применение отказоустойчивых схемотехнических решений (использование кластерных

конфигураций для серверов; двойное подключение сервера к ЛВС посредством двух сетевых интерфейсов, подключаемых к разным коммутаторам ЛВС или разным модулям одного и того же коммутатора, и др.).

В целях резервирования сетевого оборудования, средств защиты и каналов передачи данных осуществляется:

- применение отказоустойчивых схемотехнических решений;
- резервирование проводных каналов передачи данных беспроводными;
- резервирование элементов сетевого оборудования и средств защиты.

Для обеспечения возможности оперативного восстановления конфигурации серверов, сетевого оборудования и средств защиты в случае физического или логического сбоя выполняется резервное копирование конфигураций и создание образов системных дисков серверов, а также сохранение конфигурационных файлов сетевого оборудования и средств защиты.

Серверное и сетевое оборудование обеспечиваются гарантированным электропитанием.

8.4. Обеспечение безопасности сетевой инфраструктуры

В целях обеспечения непрерывного и устойчивого функционирования АСУ ТП осуществляется защита ее сетевой инфраструктуры.

Защита сетевой инфраструктуры обеспечивается:

- физической защитой сетевого оборудования и средств защиты;
- контролем логического доступа к сетевому оборудованию;
- шифрованием каналов управления;
- контролем сетевых соединений;
- обнаружением и предотвращением вторжений;
- мониторингом подключаемых к ЛВС АСУ ТП сетевых устройств;
- использованием встроенных в сетевое оборудование средств защиты от подмены адреса (средств антиспуфинга);
- защитой информации ограниченного доступа при ее передаче вне контролируемых зон;
- применением средств мониторинга и регистрации событий.

Контроль входящих и исходящих информационных потоков в ЛВС АСУ ТП осуществляется сертифицированными средствами межсетевого экранирования, размещаемыми на входе в ЛВС АСУ ТП. Контроль сетевых соединений между ЛВС

АСУ ТП и подключаемыми к ней беспроводными сетями также осуществляется средствами межсетевого экранирования.

Защита информации ограниченного доступа при ее передаче вне контролируемых зон осуществляется применением сертифицированных средств криптографической защиты информации (построением защищенных виртуальных сетей).

Защита от вторжений в ЛВС АСУ ТП осуществляется средствами обнаружения и предотвращения вторжений, размещаемыми на входе в ЛВС. Базы данных сигнатур средств обнаружения и предотвращения вторжений регулярно обновляются с сайта производителя применяемых средств.

Категорически запрещается удаленное администрирование АСУ ТП.

8.5. Защита программного обеспечения

В целях поддержания работоспособности ПО осуществляются меры по устранению уязвимостей ПО, а также другие меры защиты.

Устранение уязвимостей ПО достигается регулярным централизованным получением и установкой обновлений, предоставляемых разработчиками ПО. Обновление ОС, другого общесистемного и прикладного ПО осуществляется системными администраторами и администраторами прикладных систем.

Обновления для ПО АСУ ТП получаются с серверов обновлений, размещенных в ИУС ПХД.

Обновления ОС тестируются производителем АСУ ТП. При тестировании оценивается воздействие обновлений на функционирование АСУ ТП. Тестирование по возможности осуществляется в изолированной среде.

Для наиболее критичных систем осуществляется контроль целостности системных файлов ПО.

8.6. Регистрация и учет событий информационной безопасности

В целях своевременного выявления нарушений ИБ в АСУ ТП осуществляется контроль событий ИБ операционных и прикладных систем, СУБД, сетевого оборудования и средств защиты.

В АСУ ТП осуществляется регистрация и учет в журналах событий операционных и прикладных систем, СУБД, сетевого оборудования и средств защиты событий, которые могут быть связаны с нарушениями ИБ.

В обязательном порядке подлежат регистрации:

– действия пользователей по доступу к операционным и прикладным системам;

– действия администраторов по изменению настроек средств обработки, хранения и передачи информации, средств защиты информации, прав доступа пользователей;

– попытки несанкционированного подключения к сетевой инфраструктуре и подмены адреса сетевых устройств;

– попытки получения доступа к журналам событий.

Обеспечивается хранение журналов учета событий в течение заданного периода времени. Предусматриваются механизмы защиты журналов учета событий от переполнения, несанкционированного просмотра и изменения.

Журналы событий регулярно анализируются работниками подразделения ИБ. Для повышения эффективности контроля применяются средства анализа и корреляции событий. В целях обеспечения возможности корреляции событий осуществляется синхронизация времени всех систем с единым доверенным источником.

Перечень событий, подлежащих регистрации, период времени хранения журналов событий, периодичность контроля журналов работниками подразделения ИБ и другие меры безопасности определяются нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области ИБ.

Результаты регистрации и учета событий используются при проведении мероприятий по управлению инцидентами ИБ.

8.7. Контроль защищенности

В целях своевременного и эффективного реагирования на опубликованные и выявленные уязвимости ПО в АСУ ТП принимаются меры контроля защищенности средств обработки, хранения и передачи информации.

Контроль защищенности осуществляется специалистами отдела ИБ СКЗ. Перечень объектов контроля защищенности определяется по результатам идентификации и классификации объектов защиты, проводимой в соответствии с СТО Газпром 4.2-3-004.

Контроль защищенности осуществляется следующими способами:

– периодическим инструментальным анализом защищенности при помощи сканеров безопасности;

– анализом конфигурационных файлов средств обработки, хранения и передачи информации.

Базы уязвимостей средств контроля защищенности регулярно обновляются с сайтов производителя применяемых средств. Выявленные уязвимости средств обработки, хранения и передачи информации устраняются при помощи предлагаемых их производителями обновлений программного обеспечения или изменения конфигурации.

Все осуществляемые процедуры по контролю защищенности и устранению уязвимостей документируются.

8.8. Криптографическая защита

В целях обеспечения конфиденциальности информации при ее передаче вне контролируемых зон применяются сертифицированные установленным порядком средства криптографической защиты информации.

Процедуры управления криптографическими ключами (генерация, распределение, доступ, уничтожение) и выполнения криптографических операций, а также политика использования криптографических средств защиты определяется нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области ИБ.

8.9. Безопасность средств терминального доступа

В целях повышения уровня защищенности и устойчивости функционирования информационных систем, использующих СТД, а также предотвращения и (или) снижения возможного ущерба от инцидентов ИБ, применяются меры по обеспечению безопасности СТД.

Доступ к СТД осуществляется по принципу «запрещено все, что не разрешено явно» и только после успешного прохождения аутентификации и авторизации. Учетным записям пользователей назначаются минимальные права доступа, необходимые для выполнения служебных задач.

Для обеспечения информационной безопасности терминальных серверов, терминалов и других компонентов СТД осуществляется антивирусная защита, межсетевое экранирование, а также используются средства обнаружения вторжений.

8.10. Безопасность средств виртуализации

В целях повышения уровня защищенности и устойчивости функционирования информационных систем, использующих СВ, а также предотвращения и (или)

снижения возможного ущерба от инцидентов ИБ, применяются меры по обеспечению безопасности СВ.

Доступ к СВ осуществляется по принципу «запрещено все, что не разрешено явно» и только после успешного прохождения аутентификации и авторизации. Разграничение доступа между аппаратными платформами виртуализации, содержащими виртуальные машины, обязательно и осуществляется с использованием средств межсетевого экранирования.

Изоляция сетей информационных систем, использующих СВ, в собственные сетевые сегменты обязательна.

Для обеспечения информационной безопасности виртуальных машин и других компонентов СВ осуществляется антивирусная защита.

9. Контроль доступа

9.1. Управление доступом пользователей

В целях обеспечения безопасности информационных ресурсов и устойчивого функционирования АСУ ТП осуществляется управление доступом пользователей к операционным и прикладным системам, а также сетевому оборудованию.

Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач. Наделение пользователей правами доступа и привилегиями основывается на установленной в Обществе формализованной процедуре предоставления прав доступа. Права доступа и привилегии пользователей подлежат регулярному пересмотру.

Каждый пользователь обеспечивается уникальным персональным идентификатором. Подтверждение подлинности идентификатора (аутентификация) пользователя осуществляется при помощи паролей и/или средств усиленной аутентификации.

Длина, сложность и срок действия паролей устанавливаются в зависимости от степени критичности защищаемых систем.

9.2. Ответственность пользователей

В целях предотвращения несанкционированного доступа, а также компрометации или кражи информации и средств обработки информации,

определяется ответственность пользователей по соблюдению правил доступа при использовании АРМ.

Пользователи несут ответственность за соблюдение установленных правил при выборе и использовании паролей. Парольная политика и правила использования паролей определяются нормативными и организационно-распорядительными документами ПАО «Газпром» и Общества в области ИБ.

Пользователям запрещено работать под чужими учетными записями, а также сообщать свои пароли и передавать средства аутентификации другим пользователям.

В случае когда АРМ участвует в непрерывном производственном процессе и смена пользователя на нем повлекла бы остановку в работе системы, допускается работа нескольких пользователей под одной учетной записью.

При оставлении АРМ пользователями предпринимаются меры по защите их от несанкционированного доступа.

9.3. Контроль доступа к прикладным системам

В целях предотвращения несанкционированного доступа к информации и нарушения функционирования АСУ ТП обеспечивается контроль доступа к прикладным системам.

Доступ пользователей к информационным ресурсам (базам данных) АСУ ТП осуществляется только посредством прикладных систем. Предоставление доступа к прикладным системам осуществляется администраторами прикладных систем. Доступ пользователей к прикладным системам предоставляется после прохождения ими процедур идентификации и аутентификации.

Пользователи АСУ ТП обязаны проходить процедуру аутентификации в прикладной системе в начале каждой рабочей смены и при каждом очередном входе в нее. Предварительно может осуществляться идентификация и аутентификация в ОС. При наличии технической возможности целесообразно осуществлять единую аутентификацию в прикладных системах и ОС.

9.4. Контроль доступа к операционной системе

В целях предотвращения несанкционированного доступа к АРМ пользователей осуществляется контроль доступа к ОС.

Работа пользователей в ОС осуществляется под учетными записями с ограниченными правами. Доступ к ОС предоставляется пользователям только после прохождения процедур идентификации и аутентификации.

Управление учетными записями пользователей, их принадлежностью к группам пользователей, правами и привилегиями, а также парольной политикой осуществляется системным администратором и администратором ИБ и согласовывается с подразделением ИБ.

Средствами ОС обеспечивается автоматическое блокирование сеансов пользователей после установленного периода неактивности.

9.5. Контроль сетевого доступа

В целях предотвращения несанкционированного доступа к ЛВС АСУ ТП осуществляется контроль сетевого доступа с помощью средств межсетевого экранирования.

Конфигурация межсетевого экрана, размещаемого на входе в ЛВС АСУ ТП, предусматривает следующие основные правила:

- запрещено все, что не разрешено;
- разрешен исходящий технологический трафик в ИУС ПХД;
- разрешен входящий трафик с обновлениями, получаемыми с серверов обновлений, размещающихся в ИУС ПХД.

Дополнительные разрешающие правила обосновываются исходя из особенностей применения АСУ ТП.

Осуществляется мониторинг подключаемых к ЛВС АСУ ТП сетевых устройств в целях выявления несанкционированных подключений.

Сервисы доступа в сеть Интернет и электронной почты к использованию в АСУ ТП запрещены.

9.6. Обеспечение безопасности при использовании мобильных устройств

В целях защиты от несанкционированного доступа к ЛВС АСУ ТП и информационным ресурсам предпринимаются меры обеспечения безопасности при использовании мобильных устройств.

Для подключения к АСУ ТП используются только служебные мобильные устройства и мобильные устройства представителей разработчиков, сопровождающих АСУ ТП.

Служебные мобильные устройства являются собственностью Общества и выдаются работникам АСУ ТП по заявкам руководителей структурных подразделений для использования при выполнении ими служебных обязанностей.

Используемые служебные мобильные устройства оснащаются средствами защиты информации от несанкционированного доступа.

Перед подключением к АСУ ТП все мобильные устройства проверяются на наличие вредоносного ПО и необходимых обновлений системного ПО.

Подключение к АСУ ТП мобильных устройств разработчиков, сопровождающих АСУ ТП, и их работа осуществляются под контролем администратора ИБ (системного администратора).

Настройка и установка средств защиты на мобильные устройства возлагаются на администраторов ИБ. Контроль соответствия мобильных устройств требованиям ИБ осуществляется работниками подразделения ИБ.

При использовании беспроводных подключений к ЛВС АСУ ТП применяются меры защиты беспроводных сетей.

9.7. Обеспечение безопасности в беспроводных сетях

В целях защиты от несанкционированного доступа к ЛВС и информации в АСУ ТП обеспечивается безопасность беспроводных сетей.

Технические средства, подключаемые к ЛВС АСУ ТП по беспроводной сети, идентифицируются по физическим адресам их сетевых интерфейсов.

Подключение технических средств к беспроводной сети согласовывается с подразделением ИБ и осуществляется с обязательным прохождением процедуры аутентификации.

В беспроводных сетях осуществляется обнаружение вторжений (в том числе контроль попыток подключения к беспроводной сети).

В целях снижения вероятности несанкционированного доступа к беспроводным сетям осуществляется контроль уровня передаваемого сигнала для исключения распространения за пределы контролируемых территорий АСУ ТП.

9.8. Контроль доступа к сетевому оборудованию

В целях обеспечения безопасности сетевой инфраструктуры АСУ ТП осуществляется управление доступом администраторов к сетевому оборудованию.

Обеспечивается защита физического и логического доступа к диагностическим и конфигурационным портам сетевого оборудования.

Доступ к управлению сетевым оборудованием предоставляется только сетевым администраторам. При доступе к сетевому оборудованию применяются меры

идентификации и аутентификации. Для этого могут использоваться встроенные механизмы сетевого оборудования и сервер аутентификации.

10. Порядок пересмотра Политики информационной безопасности автоматизированной системы управления технологическими процессами

Политика ИБ АСУ ТП пересматривается с периодичностью не реже чем 1 раз в 2 года. При пересмотре Политики ИБ АСУ ТП учитываются результаты контроля эффективности обеспечения ИБ за предыдущий период.

Процедура пересмотра Политики ИБ АСУ ТП включает:

– анализ и выявление несоответствий действующей Политики ИБ АСУ ТП текущим условиям;

– разработку предложений по совершенствованию Политики ИБ АСУ ТП;

– утверждение новой редакции Политики ИБ АСУ ТП.

При осуществлении процедуры пересмотра учитываются:

– результаты контроля состояния ИБ и отзывы заинтересованных сторон о состоянии ИБ в АСУ ТП;

– изменения в организационно-штатной структуре Общества и в информационной инфраструктуре АСУ ТП;

– изменения в законодательной и нормативной базе по ИБ, произошедшие с момента утверждения предыдущей Политики ИБ АСУ ТП;

– результаты анализа произошедших инцидентов ИБ, а также уязвимости и угрозы, выявленные в АСУ ТП за время, прошедшее с момента утверждения предыдущей Политики ИБ АСУ ТП;

– изменения в управлении ИБ, включая изменения в распределении ресурсов и обязанностей при обеспечении ИБ.

Приложение А

(справочное)

Перечень документов, входящих в систему документов ООО «Газпром добыча Оренбург» в части обеспечения информационной безопасности автоматизированной системы управления технологическими процессами

Раздел Политики	Название документа
4. Общие положения	1. Политики ИБ защищаемых сервисов (процедур, процессов)
5. Принципы и направления обеспечения ИБ в АСУ ТП	2. Журнал учета объектов защиты АСУ ТП 3. Перечень средств защиты информации АСУ ТП 4. Схема ЛВС АСУ ТП
6.1. Этапы обоснования требований и разработки (модернизации)	5. Подборка документации на АСУ ТП и средств защиты информации АСУ ТП (требования по защите информации в ТЗ, проектной и эксплуатационной документации) 6. Сертификат соответствия Системы ГАЗПРОМСЕРТ
6.2. Этап ввода в эксплуатацию	7. Регламент ввода в эксплуатацию АСУ ТП 8. Акты принятия в эксплуатацию АСУ ТП и средств защиты информации АСУ ТП
6.3. Этап эксплуатации	9. Инструкции по эксплуатации АСУ ТП и средств защиты информации АСУ ТП
6.4. Этап вывода из эксплуатации	10. Регламент вывода из эксплуатации АСУ ТП
7. Физическая защита	11. Политика физической защиты объектов АСУ ТП
7.1. Защита технических средств обработки, хранения и передачи информации	12. Список лиц, допущенных в здания, сооружения и помещения, в которых размещаются критически важные технические средства АСУ ТП
7.2. Защита зданий, сооружений и помещений	13. Требования к зданиям, сооружениям и помещениям, в которых размещаются критически важные технические средства АСУ ТП
8.1. Организация безопасной эксплуатации	14. Регламент внесения изменений в оборудование и ПО АСУ ТП

средств обработки, хранения и передачи информации	15. Инструкция по установке, модификации и техническому обслуживанию ПО и аппаратных средств АСУ ТП
8.2. Защита от вредоносного программного обеспечения	16. Регламент защиты от вредоносного ПО в АСУ ТП 17. Инструкция по защите от вредоносного ПО в АСУ ТП 18. Процедуры расследования случаев проникновения и внедрения вредоносного ПО, а также восстановления систем после воздействия вредоносного ПО (в составе Регламента реагирования на инциденты ИБ и Плана обеспечения бесперебойного функционирования)
8.3. Резервирование серверов, сетевого оборудования и каналов передачи данных АСУ ТП	19. Процедуры резервирования и восстановления оборудования АСУ ТП (в Плане обеспечения бесперебойного функционирования информационной инфраструктуры Общества)
8.4. Обеспечение безопасности сетевой инфраструктуры	20. Регламент обеспечения сетевой безопасности АСУ ТП
8.5. Защита ПО	21. Инструкция по обновлению ПО АСУ ТП (может входить в Инструкцию по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АСУ ТП)
8.6. Регистрация и учет событий ИБ	22. Регламент контроля событий ИБ в АСУ ТП
8.7. Контроль защищенности	23. Регламент контроля защищенности АСУ ТП 24. Инструкция по контролю защищенности АСУ ТП
9.1. Управление доступом пользователей	25. Инструкция по организации парольной защиты в АСУ ТП
9.2. Ответственность пользователей	26. Инструкция пользователям АСУ ТП по обеспечению ИБ
9.3. Контроль доступа к прикладным системам	27. Заявки на внесение изменений в списки пользователей прикладных систем АСУ ТП и их полномочия доступа к ресурсам системы

9.5. Контроль сетевого доступа	28. Регламент управления сетевым оборудованием и средствами защиты АСУ ТП

Библиография

[1]	Политика информационной безопасности ОАО «Газпром» (утверждена приказом ОАО «Газпром» № 48 от 15.02.2008)	
[2]	СТО 25-01-2010	Политика информационной безопасности ООО «Газпром добыча Оренбург» (утверждена приказом № 285 от 27.09.2010)