ТИПОВЫЕ ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Типовые требования ИБ сформированы на основе Стандарта обеспечения информационной безопасности на стадиях жизненного цикла информационных систем и автоматизированных систем управления технологическими процессами ПАО «ГМК «Норильский никель» (С ГК НН 167-001-2020) и направлены на обеспечение защиты информации, обрабатываемой в информационной системе для которой определены:

- Класс критичности ИС, устанавливаемый требованиями Регламента идентификации и классификации информационных активов - Класс «С»;

В случае необходимости обработки в ИС информации, относящейся к другим категориям, изменений вида разрабатываемой ИС, применяемых технологий, используемых компонентов ИТ-инфраструктуры настоящие требования должны быть пересмотрены.

При создании\модернизации ИС должно быть обеспечено соответствие требованиям Стандарта обеспечения информационной безопасности на стадиях жизненного цикла информационных систем и автоматизированных систем управления технологическими процессами ПАО «ГМК «Норильский никель» (С ГК НН 167-001-2020) и законодательства РФ в сфере защиты информации, актуального для ИС.

1. Управление доступом

1.1. Требования к идентификации и аутентификации

1.1.1. При предоставлении любых видов доступа к объектам доступа КСПД обеспечивается процесс регистрации через создание учетных записей, от имени которых субъект доступа (работник, процесс, третье лицо) осуществляет доступ. К возможным видам учетных записей относятся:

- пользовательская учетная запись;
- административная учетная запись;
- техническая учетная запись (сервисная, системная, технологическая);
- коллективная учетная запись (групповая/общая);
- учетная запись третьего лица;
- специальная учетная запись (студенты и т.п.).

1.1.2. Для всех учетных записей присваиваются идентификатор и аутентификатор, при этом такой идентификатор персонифицирован и принадлежит одному субъекту доступа (за исключением технической и коллективной учетной записи).

1.1.3. Функции и назначение технических учетных записей отражаются в системном каталоге учетных записей.

1.1.4. Технические учетные записи, создаваемые при вводе в эксплуатацию ИС/эксплуатации ИС, заносятся в документ «Паспорт ИС».

1.1.5. Учетные записи специальные/третьего лица вносятся в каталог учетных записей с указанием следующих сведений и параметров:

- идентификатор учетной записи;
- ФИО пользователя;
- назначение учетной записи;

- владелец учетной записи;
- группа(ы) к которым должна принадлежать учетная запись;
- дата создания учетной записи;
- дата истечения срока действия учетной записи (в соответствии с контрактом или договором).

1.1.6. Использование коллективных учетных записей (групповых/общих) запрещается, за исключением случаев, когда их использование согласовано ДЗИиИТИ.

1.1.7. Технические учётные записи применяются только для обеспечения работы программных интерфейсов и системных служб. Интерактивный вход в систему для технических учётных записей отключен.

1.1.8. При вводе ИС в промышленную эксплуатацию пароли учетных записей, использовавшихся на стадии проектирования и реализации, изменяются администраторами соответствующих ИС.

1.1.9. Все неиспользуемые для штатной работы бизнес-приложений, инфраструктурных-приложений или компонентов ИТ-инфраструктуры учетные записи (установленные по умолчанию производителем или интегратором, тестовые и технические) удаляются или блокируются, а в случае необходимости их использования пароли для этих учетных записей изменяются. Стандартные (заводские) пароли не используются (запрещены к использованию).

1.1.10. Для автоматизированного сканирования уязвимостей (если данная функциональность поддерживается в ИС) создается учетная запись. Привилегии данной учетной записи указываются в руководстве администратора.

1.1.11. Проверка учетных данных для всех учетных записей проводится на стороне серверных компонентов ИС.

1.1.12. Механизмы аутентификации реализуются с использованием защищенных протоколов аутентификации. При хранении и передаче конфиденциальность паролей обеспечивается шифрованием или хешированием с применением стойких криптографических алгоритмов. Перечень используемых (рекомендуемых к использованию) алгоритмов шифрования приведен в Приложении И Стандарта обеспечения ИБ на стадиях жизненного цикла ИС и АСУТП ПАО «ГМК «Норильский никель» (С ГК НН 167-001-2020).

1.1.13. В процессе аутентификации в ИС пароль не отображается при его вводе, проверка введенной информации (логин, пароль) осуществляется только после полного ее ввода, в случае обнаружения ошибки, система не уточняет, какие именно данные введены неправильно.

1.1.14. Обеспечивается возможность назначения первичного пароля администратором ИС и обязательной смены пароля пользователем при первичной аутентификации в ИС.

1.1.15. Пользователям обеспечивается возможность самостоятельной установки и смены пароля.

1.1.16. Неиспользуемая в течение 90 (девяноста) дней учетная запись пользователя блокируется.

1.1.17. Обеспечивается возможность заблаговременного (не менее, чем за 14 дней) оповещения пользователей о необходимости смены пароля (посредством сообщений/подсказок или почтовых рассылок на электронные адреса пользователей).

1.1.18. Обеспечивается возможность хранения истории паролей (хэшей паролей) пользователей для предотвращения повторного их использования.

1.1.19. Обеспечивается возможность установки ограничений на параметры паролей учетных записей.

1.1.20. Пароли учетных записей: пользовательской/коллективной/третьего лица/специальной отвечают следующим требованиям:

- длина пароля составляет не менее 8 (восьми) символов;
- пароль содержит буквы в верхнем и нижнем регистрах, цифры и при необходимости специальные символы (@, #, $, &, *, % и т.п.);
- новый пароль не совпадает с тремя предыдущими;
- количество попыток неудачного ввода – не более 7 (семи), после 5 (пятой) попытки усложняющие техники вода: CAPTCHA, увеличение времени ожидания;
- время блокировки учетной записи после исчерпания лимита попыток неудачного ввода - не менее 15 (пятнадцати) минут;
- возможность копирования и вставки в поле ввода;
- срок действия пароля не более 90 (девяносто) дней;

1.1.21. Пароли учетных записей: административная/административная третьего лица отвечают следующим дополнительным к п. 1.1.20 требованиям:

- длина пароля составляет не менее 12 (двенадцати) символов;
- новый пароль не совпадает с пятью предыдущими;
- срок действия пароля не более 45 (сорока пяти) дней;

1.1.22. Пароли технических учетных записей отвечают следующим дополнительным к п. 1.1.20 требованиям:

- сгенерированы случайным образом специальными утилитами для генерации паролей;
- длина пароля составляет не менее 12 (двенадцати) символов;
- новый пароль не совпадает с пятью предыдущими;
- блокировка учетной записи после исчерпания лимита попыток неудачного ввода, без возможности автоматического разблокирования по таймауту;
- срок действия пароля не более 12 (двенадцати) месяцев;

1.1.23. Пароли учетных записей: техническая/административная/административная третьего лица должны быть отличны от всех других паролей учетных записей данного пользователя.

1.1.24. Дополнительные требования, реализуемые при внедрении или модернизации ИС:

- обеспечена возможность проверки паролей по черному списку скомпрометированных паролей, очевидных слов и комбинаций, повторяющихся/ последовательных символов, контекста (имени, фамилии пользователя, даты рождения, названия приложения и т.д.);

- осуществляется уведомление пользователя о смене/сбросе пароля, принадлежащей ему учетной записи, по электронной почте или телефону

1.2. Требования к управлению правами доступа/разделению полномочий.

1.2.1. Назначение прав доступа любых учетных записей к любым объектам доступа осуществляется в соответствии с правилом предоставления минимальных полномочий.

1.2.2. Полномочия пользователя контролируются и своевременно изменяются в соответствии кадровыми и (или) функциональными изменениями (назначение на новую должность и (или) изменение функциональных обязанностей, увольнение и т.п.).

1.2.3. Обеспечивается разграничение доступа пользователей и запускаемых от их имени процессов при их доступе к компонентам ИТ-инфраструктуры и к бизнес-приложениям с использованием соответствующих методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.

1.2.4. Обеспечивается разделение (запрет на совмещение) полномочий (ролей), выполняющих функции разработки (разработчики, проектировщики), использования (пользователи), сопровождения и эксплуатации (администраторы), эксплуатации и контроля (администраторы ИБ).

1.2.5. Реализована возможность установки срока длительности простоя (не более 15 минут) пользовательской сессии (сеанса работы), после которого сессия должна принудительно блокироваться до повторной аутентификации.

1.2.6. Обеспечивается явное ограничение или запрет на действия пользователя в ИС до прохождения процедур идентификации и аутентификации. В частности, пользователю не выдается информация о типе и версии ИС или ее компонентов до успешного завершения процедур аутентификации.

1.2.7. Запрещён по умолчанию прямой доступ пользователей, администраторов, третьих лиц в продуктивные базы данных ИС.

1.2.8. Хранение и обработка информации Компании/РОКС НН (за исключением общедоступной) с применением внешних (функционирующих вне КСПД и ТСПД) облачных сервисов запрещена.

2. Сбор и анализ событий ИБ

2.1. Выполняется синхронизация системного времени компонентов ИТ-инфраструктуры с корпоративным NTP-сервером (допустимая погрешность не более 5 (пяти) сек).

2.2. Обеспечивается возможность регистрации следующих событий безопасности в системных компонентах и бизнес-приложениях (как минимум, но не ограничиваясь):

- факты или попытки идентификации и аутентификации субъектов доступа;
- факты изменения полномочий, модификация профиля пользователей;
- факты создания, изменения или блокирования учетных записей;

- действия привилегированных пользователей и администраторов по настройке и изменению конфигурации ИС (в том числе изменение настроек аудита);
- факты запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации);
- факты доступа к защищаемым объектам доступа (включая журналы регистрации событий и параметры конфигурирования);
- факты создания и удаления и изменения объектов системного уровня (исполняемые файлы, таблицы баз данных, хранимых процедур, журналов регистрации событий).

Допускается изменение перечня регистрируемых событий при обязательном согласовании таких изменений с ДЗИиИТИ.

2.3. Обеспечивается фиксация следующей информации для каждого регистрируемого события безопасности:

- тип события безопасности;
- дата и время события безопасности;
- идентификационная информация источника события безопасности;
- результат события безопасности (успешно или неуспешно);
- субъект доступа (пользователь и (или) процесс и объект доступа, связанный с данным событием безопасности)

2.4. Обеспечивается хранение информации о событиях безопасности в журналах регистрации событий ИС в течение не менее 3 (трех) месяцев.

2.5. Обеспечивается ограничение доступа к журналам регистрации событий безопасности только уполномоченным пользователям.

2.6. Журналы регистрации событий не должны содержать информационных активов, которым присвоена категория ПДн, ИИ или КТ.

2.7. Администраторами ИС осуществляется контроль настроек журналов регистрации событий безопасности и аудита.

2.8. В ИС осуществляется регистрация информации о типе и версии мобильного клиента/браузера, используемого для получения доступа к ней.

3. Сетевая безопасность

3.1. Сетевая безопасность

3.1.1. Сегментация по зонам безопасности обеспечивается исходя из принципов физического или логического разделения.

3.1.2. Взаимодействие технических средств, подключенных к КСПД, сервисов, систем и приложений КСПД с объектами доступа в иных сетях (внешних по отношению к КСПД) обеспечивается строго через демилитаризованную зону КСПД.

3.1.3. Разработаны и внедрены правила МЭ и определены правила сетевой фильтрации на основе анализа адресов источника и получателя передаваемой информации, сетевых протоколов, сетевых портов и иных значимых параметров сетевых

пакетов. Правилами сетевой фильтрации обеспечивается разграничение доступа на уровне пользовательских сущностей в соответствии с правилом предоставления минимальных полномочий. Контроль сетевого трафика обеспечивается по принципу белого списка - разрешенный сетевой трафик указывается явно, остальной трафик блокируется.

3.1.4. Взаимодействие компонентов одной или нескольких ИС осуществляется с использованием защищенных протоколов передачи данных в доверенной зоне КСПД. Организация взаимодействия нескольких ИС выполняется с использованием ресурсов корпоративной системы интеграции приложений (КСИП).

3.1.5. Для интегрируемых ИС предусмотрена учетная запись, от имени которой осуществляется ограниченный доступ к передаваемым данным и функциям интеграционного взаимодействия. Права такой учетной записи являются минимально необходимыми для обеспечения интеграционного взаимодействия.

3.1.6. Для обеспечения контроля интеграционного взаимодействия при интеграции ИС с другими ИС Компании выполняется тестирование полноты реализации требований ИБ, применимых в данной ИС в соответствии с настоящим Стандартом.

3.2. Требования к защите удаленного доступа

3.2.1. Удаленный доступ предоставляется только с использованием защищенных протоколов и технологий удаленного доступа, использующих рекомендованные криптографические алгоритмы (состав рекомендованных к применению протоколов и алгоритмов шифрования приводятся в Приложении И Стандарта обеспечения ИБ на стадиях жизненного цикла ИС и АСУТП ПАО «ГМК «Норильский никель» (С ГК НН 167-001-2020)). Удаленный доступ предоставляется только после прохождения процедур идентификации и аутентификации пользователя.

3.2.2. Удаленный доступ предоставляется только при использовании следующих технологий:

- терминальный доступ или доступ с использованием технологии VDI (Virtual Desktop Infrastructure). При таком доступе используются технологии Microsoft RDS и Vmware Horizon (для виртуальной инфраструктуры);
- доступ с использованием VPN. При таком доступе используется клиентское ПО – Cisco Any Connect.

3.2.3. Удаленный доступ для третьих лиц (подрядчиков, разработчиков) предоставляется только на основании заключенного контракта, в том числе содержащего соглашение о неразглашении к получаемой информации, и только в рамках выполняемых третьим лицом работ и задач. По умолчанию набор полномочий при удаленном доступе не соответствует набору полномочий доступа для пользователей внутри КСПД.

4. Криптографическая защита информации

4.1. Требования к шифрованию сетевого трафика

4.1.1. Обеспечивается криптографическая защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи. При использовании методов шифрования используются рекомендованные алгоритмы шифрования, приведенные в Приложении И Стандарта обеспечения ИБ на стадиях жизненного цикла ИС и АСУТП ПАО «ГМК «Норильский никель» (С ГК НН 167-001-2020). При отсутствии технической возможности использования рекомендованных алгоритмов шифрования передача данных обеспечивается только в доверенной зоне КСПД или с применением наложенных СКЗИ.

4.1.2. Обеспечивается защита идентификационной и аутентификационной информации при использовании рекомендуемых протоколов для защиты сетевых соединений, контроля целостности и шифрования данных, приведенных в Приложении И Стандарта обеспечения ИБ на стадиях жизненного цикла ИС и АСУТП ПАО «ГМК «Норильский никель» (С ГК НН 167-001-2020). При отсутствии технической возможности использования рекомендованных протоколов обеспечивается передача данных только в доверенной зоне КСПД или с применением наложенных СКЗИ.

4.1.3. Защита каналов связи обеспечивается путем применения сертифицированных СКЗИ. СКЗИ, не прошедшие оценку соответствия требованиям по безопасности в форме обязательной сертификации, используются только для организации удаленного доступа.

4.2. Требования к сертификатам ключей проверки ЭП

4.2.1. Сертификат ключа проверки ЭП соответствует формату X.509 на базе алгоритма RSA, требования приведены в Приложении К Стандарта обеспечения ИБ на стадиях жизненного цикла ИС и АСУТП ПАО «ГМК «Норильский никель» (С ГК НН 167-001-2020).

4.2.2. Для внутрикорпоративного УЦ длина ключа RSA составляет не менее 2048 бит.

5. Ограничение программной среды

5.1. Требования к контролю установки ПО

5.1.1. На компоненты ИТ-инфраструктуры устанавливается только разрешенное к использованию ПО. Примечание: Разрешенным к применению считается ПО, входящее в комплект штатной поставки системного ПО, прикладное ПО, необходимое для выполнения установленных бизнес-функций, а также ПО, согласованное к установке ДЗИиИТИ/Службой ИБ.

5.1.2. Установка средств разработки (отладчики, компиляторы и т.п.) на продуктивные экземпляры ИС запрещена.

5.1.3. Все компоненты и прикладное ПО на этапе передачи ИС в промышленную эксплуатацию реализованы с использованием стабильных сборок ПО, включают

все необходимые обновления, обеспечивающие максимальную защищенность ИС (отсутствие известных технических уязвимостей).

6. Управление конфигурациями

6.1. Выполняется настройка (конфигурирование) всех компонентов ИТ-инфраструктуры и ИС, обеспечивающая наибольшую защищенность в соответствии с требованиями Компании (методическими указаниями по конфигурированию), рекомендациями производителей и специализированных организаций.

6.2. Формируются и применяются базовые образы и типовые конфигурации АРМ, сетевого оборудования, серверного оборудования (в том числе, виртуальных машин), включающих ОС, базовый пакет ПО, сервисное ПО, СЗИ. Базовые образы и типовые конфигурации согласовываются с ДЗИиИТИ/Службой ИБ.

6.3. Эксплуатация ИТ-инфраструктуры КСПД в режимах работы по умолчанию от производителя (default mode) и преднастроенных режимах без их адаптации под требования ИБ Компании исключена. В том числе, запрещено использование конфигурации активного сетевого/телекоммуникационного оборудования и СЗИ с параметрами по умолчанию от производителя.

7. Управление техническими уязвимостями ИБ

7.1. Осуществляется выявление, анализ уязвимостей ИТ-инфраструктуры, ИС и их оперативное устранение.

7.2. Осуществляется контроль установки обновлений ПО, включая обновление СЗИ.

7.3. Все применимые обновления безопасности компонентов ИС и ее СЗИ устанавливаются в течение рекомендуемого производителем срока с момента их выпуска.

7.4. Получение обновлений безопасности осуществляется только из доверенных источников.

7.5. Перед установкой обновлений проводится их тестирование на тестовой группе перед их тиражированием на все ИС.

7.6. Производится отключение неиспользуемых сервисов на технических средствах, подключенных к КСПД.

7.7. Производится блокирование возвращаемых приглашений (баннеров), однозначно идентифицирующих сервисы с целью уменьшения периметра перечисления сервисов и ОС.

8. Управление инцидентами ИБ

8.1. Обеспечивается обнаружение, идентификация и регистрация инцидентов ИБ на основе сбора, обработки и корреляции событий безопасности, получаемых от различных компонентов ИС.

8.2. Обеспечивается своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов ИБ пользователями и администраторами.

8.3. Регламентирован и проводится анализ инцидентов ИБ, в том числе определяются источники и причины возникновения инцидентов ИБ, а также проводится оценка их последствий.

8.4. Принимаются меры по устранению последствий инцидентов ИБ.

8.5. Планируются и принимаются меры по предотвращению повторного возникновения инцидентов ИБ.

9. Требования к резервному копированию и восстановлению

9.1. Выполняется резервное копирование конфигураций ИС на защищенные ресурсы с ограниченным доступом.

9.2. Для ИС предусматриваются механизмы резервного копирования и восстановления данных.

9.3. Обеспечивается хранение резервных копий журналов безопасности не менее 6 месяцев.

9.4. Обеспечивается периодическое тестирование резервных копий и возможности восстановления в случае нештатных ситуаций.

10. Защита от вредоносного ПО

10.1. Реализуется защита от вредоносного ПО (включая защиту от технологий мобильного кода) всех компонентов ИТ-инфраструктуры, подверженных воздействию вредоносного ПО или способных быть источником распространения вредоносного ПО, в том числе:

- АРМ пользователей;
- файловые, почтовые, web-серверы, серверы обновлений, сервера резервного копирования и др.

10.2. Осуществляется обновление базы данных признаков вредоносного ПО на регулярной основе (не реже чем раз в 24 (двадцать четыре) часа).

11. Состав основных требований к документированию

11.1. Определены и подписаны договора (контракты) и соглашения о неразглашении информации при доступе третьих лиц к конфиденциальной информации (тестовым данным, сведениям о технологиях обработки и защиты информации и т.п.) Компании. В договор с третьими лицами включены требования ИБ, в том числе требования к управлению доступом.

11.2. Разработана Пояснительная записка к техническому проекту в части раздела по реализации требований ИБ / Проектное решение по информационной безопасности.

11.3. Разработана Схема структурная комплекса технических средств (возможно в составе Пояснительной записки / Проектного решения по информационной безопасности).

11.4. Разработано Описание комплекса технических средств и описание ПО (возможно в

качестве приложения к Пояснительной записке / Проектному решению по информационной безопасности).

11.5. Разработана спецификация приобретаемых технических средств и ПО СЗИ.

11.6. Разработано (представлено) Руководство по эксплуатации СЗИ, непосредственно входящих в состав ИС.

11.7. Разработана Концепция ролей и полномочий. Описание ролей и требуемых полномочий, в том числе (в составе единого документа Правила доступа):

- общее понятие прав доступа;
- описание объектов полномочий;
- реестры ролей (роли бизнес пользователей, роли пользователей поддержки, роли ИБ):
- название роли;
- техническое наименование роли в ИС;
- краткое описание роли;
- владелец;
- классификация ролей по доступу к КТ, ИИ, ПДн;
- реестр технических/служебных учетных записей с указанием владельцев;
- реестр полномочий;
- правила разграничения доступа (с описанием как работают правила, можно сделать скриншоты с описанием работы правил);
- матрица ролей и полномочий пользователей в ИС;
- матрица конфликтов бизнес–ролей;
- реестр рисков разделения полномочий;
- технические правила разделения полномочий.

11.8. Разработаны Правила предоставления доступа в том числе описание порядка предоставления доступа пользователей в ИС (в составе единого документа Правила доступа):

- описание ландшафта ИС;
- порядок создания, блокирования учетной записи;
- порядок предоставления/блокировки доступа к продуктивной среде, включая маршрут согласования;
- порядок предоставления/блокировки доступа к тестовой среде и среде разработки (если применимо), включающий маршрут согласования;
- ограничения и допущения при предоставлении прав доступа (включая удаленный доступ);
- шаблон заявки на предоставление/блокировку доступа.

11.9. Разработано описание основных обязанностей и правил работы пользователя в части обеспечения ИБ (в составе Руководства пользователя):

- проверка пользователями готовности рабочего места к подключению к ИС;
- основные обязанности пользователей в части обеспечения ИБ;
- порядок авторизации пользователей в ИС;
- ограничения действий пользователей в части ИБ;
- окончание работы с ИС (временное покидание рабочего места);

- действия пользователей в случае обнаружения ошибок и сбоев, инцидентов.

11.10. Разработано Руководство администратора в том числе описание действий администратора по настройке и контролю параметров безопасности:

- перечень функциональных обязанностей администратора ИС в части ИБ;
- порядок и параметры настройки мер по защите информации;
- порядок проведения аудита в части ИБ.

11.11. Разработан План аварийного восстановления в том числе описание порядка технического обслуживания системы в части ИБ, восстановления работоспособности и функционирования мер по защите информации, а также проведения резервного копирования и восстановления данных ИС.

11.12. Разработаны Программа и методики испытаний в целях подтверждения выполнений требований по ИБ, включая:

- проверку соответствия состава и размещения ТС ИС проектным решениям;
- проверку выполнения организационных требований по ИБ;
- оценку полноты разработки организационно-распорядительной, проектной и эксплуатационной документации (сценарий проверки соответствия содержания представленных документов установленным требованиям);
- проверку ИС на соответствие установленным требованиям по ИБ.

11.13. Разработаны:

- Протокол предварительных испытаний;
- Протокол приемочных испытаний;
- Акт ввода ИС в промышленную эксплуатацию.

11.14. Разработан Паспорт ИС в соответствии с принятым в Компании шаблоном.