

Стандарт предприятия

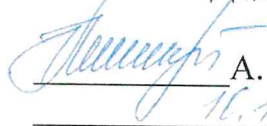
Управление доступом к информационным ресурсам ИС

Введен впервые

УТВЕРЖДАЮ

Генеральный директор

ООО «Эн+ Диджитал»

 А. А. Герасименко
10.10.2018

(дата)

Введен в действие приказом

ООО «Эн+ Диджитал»

от 08.10.18г. № 23

ООО «Эн+ Диджитал»

Содержание

Содержание	2
Область применения	3
2. Нормативные ссылки	3
3. Сокращения и определения	3
4. Общие сведения	4
5. Основные положения	4
6. Порядок предоставления доступа к информационным ресурсам/системам	5
7. Порядок отмены доступа к информационным ресурсам/системам	6
8. Порядок изменения прав доступа к информационным ресурсам/системам	6
9. Порядок актуализации разграничения прав доступа к информационным ресурсам/системам	6
10. Контроль	7
11. Ответственность	7
Лист регистрации изменений	10

Область применения

1.1. Настоящий стандарт предприятия устанавливает:

1.1.1. порядок предоставления работникам ООО «Эн+ Диджитал» (далее Компании) и прочим лицам доступа к информационным ресурсам/системам Компании, включая сетевые сервисы (сервис печати, электронная почта, Web-серверы и т. д.), разделяемые сетевые файловые ресурсы (файлы, каталоги, диски, рабочие станции, периферия), серверы баз данных и т. п.;

1.1.1. порядок отмены доступа увольняемых работников Компании и прочих лиц к информационным ресурсам/системам;

1.1.2. порядок изменения прав доступа пользователей при переходе на другую должность, изменении должностных обязанностей и т.п.;

1.1.3. требования, предъявляемые к работникам Компании и прочим лицам в связи с предоставлением им доступа к информационным ресурсам/системам;

1.1.4. порядок осуществления контроля выполнения положений настоящего стандарта;

1.1.5. ответственность работников Компании и прочих лиц за нарушение требований, устанавливаемых настоящим стандартом.

1.2. Настоящий стандарт предприятия распространяется на всех работников Компании (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.), зарегистрированных в ИС Компании в порядке, устанавливаемом настоящим стандартом, и получивших права на доступ к информационным ресурсам/системам в соответствии с функциональными обязанностями.

1.3. Настоящий стандарт предприятия входит в состав нормативных документов системы управления Компании.

2. Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие документы:

- СТП 006-2018 «Управление паролями».

3. Сокращения и определения

3.1. В настоящем стандарте используются следующие сокращения:

ИБ - информационная безопасность;

ИТ – информационные технологии;

ИС – информационная система.

3.2. В настоящем стандарте используются следующие определения:

Компания ООО «Эн+ Диджитал», а также партнеры, являющиеся пользователями или администраторами информационных систем ООО «Эн+ Диджитал», подписавшие соответствующие соглашения.

Подразделения ИБ – подразделение (работник), ответственное за контроль обеспечения ИБ Компании, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.

ИТ служба – подразделение (работник) Компании, осуществляющее функции ИТ обеспечения Компании, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.

Учетная запись – описание пользователя, которое хранится в информационных системах. Обычно включает в себя логин, настоящее имя, пароль права пользователя.

Логин – имя пользователя в информационной системе.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора (логина учетной записи); подтверждение подлинности.

Идентификация – присвоение субъектам и объектам доступа идентификатора (учетной записи) и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Запрос на предоставление/изменение/отмену прав доступа – обращение установленного образца в системе учета запросов Компании.

Пользователи информационной системы – все работники Компании (штатные, временные, работающие по контракту и т.п.), а также все прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в ИС Компании в порядке, устанавливаемом настоящим стандартом, и получившие права на доступ к информационным ресурсам/системам в соответствии с функциональными обязанностями.

4. Общие сведения

4.1. В информационных системах Компании хранится и обрабатывается информация Компании, являющаяся жизненно важной для ведения бизнеса.

4.2. С целью обеспечения защиты информационных ресурсов, входящих в ИС Компании от их незаконного использования, утечки конфиденциальной информации, умышленного или неосторожного нарушения целостности или доступности критичной информации и других угроз информационной безопасности настоящим стандартом устанавливается единый для всех порядок предоставления, изменения и отмены доступа пользователей к информационным ресурсам и соответствующие требования безопасности, обязательные для всех пользователей.

5. Основные положения

5.1. Доступ к информационным ресурсам/системам должен осуществляться зарегистрированными пользователями ИС при предъявлении доказательств их подлинности (идентификация и аутентификация). Используемая схема аутентификации должна быть устойчива к несанкционированному прослушиванию каналов связи.

5.2. В Компании должен использоваться единый сквозной механизм аутентификации в ИС, прозрачный для пользователя. Если в ИС это требование реализовать невозможно, тогда используемый в ней механизм аутентификации согласуется с Подразделением ИБ.

5.3. Для предоставления работникам Компании и всем прочим лицам доступа к информационным ресурсам/системам должна осуществляться процедура их регистрации в качестве пользователей ИС. В результате регистрации каждому пользователю создается одна или несколько учетных записей, используемых для получения доступа к локальному компьютеру, сетевым сервисам (сервис печати, электронная почта, Web-серверы и т. д.), разделяемым сетевым файловым ресурсам (файлы, каталоги, диски, рабочие станции, периферия), серверам баз данных и т. п.

5.4. Учетные записи пользователя включают в себя данные - логины, однозначно идентифицирующие данного пользователя, и служат для определения пользовательских полномочий по доступу к информационным ресурсам, а также осуществления контроля над действиями пользователей. Исключение составляют случаи использования общих учётных записей. Однако при использовании общих учётных записей должна обязательно иметься иная возможность сопоставления сеанса работы под такой учётной записью с конкретным пользователем (сопоставление с учётной записью входа в операционную систему, журналы и графики дежурств, средства видеоконтроля помещений и т.д.).

5.5. Для проведения автоматизированных операций в ИС возможно использование выделенных учетных записей - системных записей. Идентифицирующие данные такой

записи используются работниками ИТ службы по согласованию с владельцами.

5.6. Учетные записи пользователей ИС с расширенными правами - административные записи, должны входить в утвержденный владельцем общий перечень пользователей.

5.7. При наличии технической возможности и при согласовании Подразделения ИБ владелец информационного ресурса/системы назначает работника из своего структурного подразделения, который производит изменения прав доступа самостоятельно без участия ИТ службы.

5.8. Не допускается использование логинов учетных записей других пользователей для осуществления доступа к информационным ресурсам.

5.9. Всем пользователям присваивается уникальное имя (логин) и пароль. Пароль служит доказательством того, что пользователь является именно тем, за кого себя выдает. Пароль пользователи обязаны держать в секрете и никому не сообщать.

5.10. При переводе работника между подразделениями Компании, необходимо производить последовательно: отмену доступа (пункт 7 данного стандарта), предоставление доступа (пункт 6 данного стандарта).

5.11. При изменении фамилии, имени или отчества работника учетная запись пользователя изменяется для приведения в соответствие с официальными документами. Допускается оставлять старые реквизиты работника в наименовании учетной записи при наличии обоснования и согласовании Подразделения ИБ.

5.12. При выборе, хранении и использовании паролей пользователи должны руководствоваться правилами СТП 006-2018 «Управление паролями».

5.13. Все запросы на предоставление или изменение прав доступа к информационным ресурсам/системам должны регистрироваться в системе учета заявок Компании.

5.14. Запрос на предоставление/ изменение/ отмену доступа должен содержать: ФИО работника/внешнего пользователя, наименование подразделения или организации где он работает, его должность, логин учетной записи пользователя, наименование информационного ресурса/системы, вид доступа/роль, период. Далее указывается обоснование необходимости выполнения данного запроса. Дополнительно могут указываться уточняющие сведения для корректной и безопасной настройки прав доступа: адрес расположения автоматизированного рабочего места (если оно располагается за пределами корпоративной информационно-вычислительной сети), наименование автоматизированного рабочего места/IP (если известно, как оно называется). Примерная форма запросов приведена в Приложении 1.

6. Порядок предоставления доступа к информационным ресурсам/системам

6.1. Права доступа к информационным ресурсам/системам предоставляются пользователю на время и в объеме, необходимом для выполнения им своих должностных обязанностей.

6.2. Первоначальный доступ к информационным ресурсам/системам предоставляется работнику Компании, когда он приступает к должностным обязанностям, только после ознакомления с документами (политики, стандарты, инструкции, регламенты, документация), регламентирующими правила работы пользователей в ИС.

6.3. Доступ к информационным ресурсам предоставляется только на основании запроса установленной формы, направленного в ИТ службу и подписанного руководителем структурного подразделения работника. Для прочих лиц, не являющихся работниками Компании, запрос на предоставление доступа оформляет руководитель подразделения функционально ответственного за взаимодействие с этими лицами.

6.4. Для предоставления доступа к конкретным информационным ресурсам/системам Компании инициатор запроса в обязательном порядке предоставляет требуемые

согласующие подписи руководителей подразделений, владеющих этими ресурсами/системами.

6.5. На основании полученных на исполнение запросов работник подразделения ИТ обязан создать учетные записи (при необходимости) и произвести назначение запрашиваемых на указанный срок полномочий.

7. Порядок отмены доступа к информационным ресурсам/системам

7.1. После подачи работником заявления об увольнении (или прекращения работ иных лиц в Компании) его руководитель определяет дату отмены доступа с учетом соблюдения мер по обеспечению информационной безопасности Компании. Если отмена необходима до даты увольнения, то руководитель направляет в ИТ службу запрос об отмене пользователю доступа к информационным ресурсам/системам Компании, в ином случае учетная запись блокируется (отключается) в день последующий за датой увольнения работника.

7.2. В случае длительного неиспользования работником учетной записи (отпуск по уходу за ребенком, продолжительная болезнь, очень редкая необходимость использования и проч.), его руководитель вправе направить запрос в ИТ службу о необходимости ее блокировки и сохранения для дальнейшего использования.

7.3. Отдел кадров обязан направить уведомление в ИТ службу и подразделение ИБ об увольнении работника не позднее даты увольнения.

7.4. Работники ИТ службы обязаны произвести блокировку всех учетных записей данного работника или иного лица (в сетевых доменах, почтовых системах, приложениях, сервере удаленного доступа, серверах баз данных и т.п.) по запросу, полученному от руководителя структурного подразделения, либо не позднее одного дня после получения уведомления об увольнении работника от отдела кадров.

7.5. Заблокированная пользовательская учетная запись должна удаляться через 6 месяцев после блокировки, за исключением случаев, описанных в п.7.2.

8. Порядок изменения прав доступа к информационным ресурсам/системам

8.1. В случае изменения должностных обязанностей работника, перевода на другую должность, в другое подразделение и т.п., его руководитель подаёт в ИТ службу запрос на изменение прав доступа пользователя к информационным ресурсам/системам.

8.2. В запросе указываются сведения в соответствии с пунктом 5.13 настоящего стандарта и (при необходимости) выполняется процедура отмены полномочий, описанная в разделе 7 настоящего стандарта, назначенных пользователю ранее.

8.3. Назначение прав доступа пользователей к информационным ресурсам/системам производится в соответствии с Порядком предоставления доступа, описанным в разделе 6 настоящего стандарта.

8.4. Работники ИТ службы производят изменение прав доступа к ресурсу/системе по запросу, полученному от руководителя структурного подразделения не позднее одного дня после получения запроса.

8.5. При наличии в запросе пункта об отмене назначенных пользователю ранее прав доступа к информационным ресурсам/системам, перед назначением пользователю новых прав доступа работник ИТ службы обязан ликвидировать ранее назначенные права доступа.

9. Порядок актуализации разграничения прав доступа к информационным ресурсам/системам

9.1. Отдел кадров должен ежемесячно уведомлять подразделение ИБ и ИТ службу об уволенных/переведенных в течение последнего месяца работников.

9.2. Ежемесячно подразделение ИТ выявляет регистрационные записи, не

используемые пользователями более полугода и блокирует их.

9.3. Владельцы информационных ресурсов/систем ежегодно до 1 марта должны совместно с подразделением ИТ уточнять списки доступа к их ресурсам/системам.

9.4. ИТ подразделение должно проводить актуализацию списка доступа работников к ресурсам по данным предоставленным отделом кадров и владельцами.

9.5. При нахождении расхождений требуемого и установленного уровня доступа ИТ служба уведомляет владельца информационного ресурса/системы. По результатам актуализации владелец информационного ресурса/системы направляет новые списки доступа в ИТ службу для настройки прав.

9.6. Для приведения доступа в соответствии с требованиями владелец информационного ресурса/системы выполняет процедуры разделов 6-8 настоящего СТП.

10. Контроль

10.1. Контроль выполнения требований настоящего стандарта осуществляется работниками Подразделения ИБ путем регулярного проведения аудита системы управления доступом (предоставления, изменения, отмены и использования прав доступа) к информационным ресурсам/системам Компании, регистрации событий, связанных с получением доступа к ним, а также при проведении аудитов информационной безопасности.

10.2. Работники ИТ службы осуществляют регулярный анализ журналов регистрации событий, происходящих в информационных системах с целью выявления попыток обхода механизмов защиты информации и получения несанкционированного доступа к информационным ресурсам/системам Компании.

10.3. С целью своевременного выявления уязвимостей системы защиты информационных ресурсов/систем Компании и предупреждения возможных нарушений информационной безопасности, работниками Подразделения ИБ проводятся проверки уровня защиты информационных ресурсов/систем с использованием средств и методов анализа защищенности с имитацией действий потенциального злоумышленника по осуществлению несанкционированного доступа к информации.

10.4. Работники Подразделения ИБ вправе требовать устранения выявленных замечаний по ИБ и незамедлительного реагирования на них от работников, в том числе ИТ службы.

10.5. В Компании применяются средства контроля доступа и другие меры защиты для обеспечения конфиденциальности, целостности и доступности информации, обрабатываемой в информационных системах. С этой целью ИТ службе предоставляются следующие функции:

10.5.1. ограничивать или отменять полномочия любого пользователя;

10.5.2. проверять, копировать, удалять или иным способом изменять любые данные, программы и другие системные ресурсы, из-за которых обеспечение защиты информации может оказаться недостижимым;

10.5.3. предпринимать любые другие действия, необходимые для обеспечения информационной безопасности ресурсов/систем Компании.

10.6. Перечисленные выше действия могут осуществляться как с уведомлением руководства пользователей, которых затрагивают эти изменения, так и без такового при согласовании с Подразделением ИБ Компании.

10.7. По всем фактам, связанным с нарушением требований настоящего стандарта и представляющим угрозу для информационной безопасности Компании, Подразделением ИБ проводятся служебные расследования.

11. Ответственность

11.1. Ответственность за осуществление контроля выполнения требований

настоящего стандарта, а также за поддержание данного документа в актуальном состоянии несет Менеджер ИБ.

11.2. Ответственность за соблюдение работниками ИТ службы порядка предоставления (изменения, отмены) доступа к информационным ресурсам/системам Компании, устанавливаемого настоящим стандартом, и организацию учета запросов на предоставление (изменение, отмену) доступа возлагается на руководителя ИТ службы.

11.3. Руководители подразделений Компании несут ответственность за определение уровня полномочий, запрашиваемых для предоставления их подчиненным доступа к информационным ресурсам/системам Компании в строгом соответствии с их должностными обязанностями.

11.4. Исполненные запросы на предоставление (изменение, отмену) доступа пользователя должны храниться в системе учета запросов Компании в течение всего периода работы пользователя в Компании, а также в течение трех лет после его увольнения (или завершения работ).

11.5. Лица, нарушающие требования настоящего стандарта, несут ответственность в соответствии с нормами действующего законодательства Российской Федерации.

Лист согласования**СОГЛАСОВАНО:**

Структурное подразделение, должность	Подпись	Фамилия И.О.	Дата

РАЗРАБОТЧИК:

Должность	Подпись	Фамилия И.О.	Дата
Исполнительный директор		Шевченко Д.А.	

Лист регистрации изменений

Порядковый номер изменения	Основание ¹	Срок введения изменения	Изменения внёс			Примечания
			ФИО	Подпись	Дата внесения изменения	

¹ Ссылка на документ, разрешающий внесение изменений и содержащий тест изменений.

Запрос для первоначального доступа.

Об организации рабочего места
принимаемого /перемещаемого работника
/внешнего пользователя

<Вариант 1>

Прошу предоставить /изменить /отменить доступ:

1. ФИО: Иванов Савелий Петрович;
2. Название структурного подразделения/организации: ЦТАИ ТЭЦ-14;
3. Наименование должности: инженер 1 категории;
4. Учетная запись пользователя: ivanov_sp;
5. Наименование информационного ресурса/системы: АСУ ЦК;
6. Вид доступа/роль: Цех;
7. Рег.запись ПК/IP¹: ivanov_sp (192.168.30.45).

на срок с «__» _____ 201__ по «__» _____ 201__ года/ на весь период работы.

<Обоснование необходимости выполнения данного запроса>

Руководитель подразделения

/ _____

Визовый блок:

<Указываются визы владельцев информационных ресурсов/систем к которым запрашивается доступ.>

¹ Необязательное поле

<Вариант 2>

Прошу предоставить доступ:

№	ФИО	Название структурного подразделения/ организации	Наименование должности	Рег.запись пользователя	Наименование информационного ресурса/системы	Вид доступа/ роль	Рег.запись ПК/IP ³	Адрес автоматизированного рабочего места*	Период
1	Иванов Савелий Петрович	ЦТАИ ТЭЦ-14	Инженер I категории	Tec14\ Ivanov_sp	АСУ ЦК	Цех	Ivanov_sp (192.168.30.45)	-	на весь период работы
2	Сидоров Павел Иванович	Руководство ТЭЦ-14	Директор	TEC14\ Sidorov_P1	КИВС (почта, КСУ)	VPN	Nb_Sidorov_P1	-	на весь период работы
4	Петров Илья Сергеевич	ООО «Энергосервис-монтаж»	Консультант	ID\ Petrov_IS	КИВС (192.168.31.3 – сервер учета оборудования)	VPN	FireWall-ESM (10.85.40.53)	г. Москва, ул. Строителей, д. 43	18.03.2013 – 23.06.2013

Отменить доступ:

№	ФИО	Название структурного подразделения/ организации	Наименование должности	Рег.запись пользователя	Наименование информационного ресурса/системы	Вид доступа/ роль	Рег.запись ПК/IP*	Адрес автоматизированного рабочего места*	Период
1	Иванов Савелий Петрович	ЦТАИ ТЭЦ-14	Инженер I категории	Tec14\ Ivanov_sp	АСУ ЦК	Просмотр	Ivanov_sp (192.168.30.45)	-	с 20.03.2013
2									

<Обоснование необходимости выполнения данного запроса>

Руководитель подразделения

Визовый блок:

<Указываются визы владельцев информационных ресурсов/систем к которым запрашивается доступ.>

³ Необязательное поле