

# Стандарт предприятия

---

## План обеспечения непрерывности бизнеса

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
Введение .....	<b>Ошибка! Закладка не определена.</b>
1. Область применения .....	3
2. Нормативные ссылки .....	3
3. Сокращения и определения .....	3
4. Общие положения .....	4
5. Цели и задачи .....	4
6. Основные требования .....	5
7. Рабочие группа по ликвидации последствий аварии Функциональные обязанности и ответственность .....	6
8. Определение приоритетов для прикладных систем .....	8
9. Средства обеспечения непрерывной работы и восстановления .....	8
10. Резервный вычислительный центр .....	9
11. Тестирование плана .....	9
12. Сопровождение плана .....	10
13. Ответственность .....	10
Лист регистрации изменений .....	12

## 1. Область применения

1.1. Настоящий стандарт предприятия определяет общие подходы и систему мер, предпринимаемых в ООО «Эн+ Диджитал» (далее Компания) для обеспечения бесперебойной деятельности КИВС.

1.2. Настоящий стандарт предприятия распространяется на все подразделения ООО «Эн+ Диджитал».

1.3. Настоящий стандарт предприятия входит в состав нормативных документов системы управления ООО «Эн+ Диджитал».

## 2. Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие документы:

- СТП 001-2018 «Политика в области информационной безопасности».
- СТП 007-2018 «Система резервного копирования и восстановления информационных ресурсов КИВС».

## 3. Сокращения и определения

3.1. В настоящем стандарте используются следующие сокращения:

**ИТ** – информационные технологии;

**КИВС** – корпоративная информационно-вычислительная сеть;

**ОВЦ** – основной вычислительный центр;

**РВЦ** – резервный вычислительный центр;

**ПО** - программное обеспечение

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.

**Информационные ресурсы (активы)** - Информационные ресурсы (активы) Компании включают в себя информацию, напечатанную или записанную на бумаге, пересылаемую по почте или демонстрируемую в видеозаписях, передаваемую устно, информацию, хранимую в электронном виде на серверах, веб сайтах, мобильных устройствах, магнитных и оптических носителях и т.п., а также информацию, обрабатываемую в корпоративных информационных системах и передаваемую по каналам связи. Информационные ресурсы Компании также включают в себя программное обеспечение: операционные системы, приложения, утилиты, программную документацию и т.п.

**Информационная безопасность** - Защита информации (информационных ресурсов, активов) от широкого спектра угроз (в отношении конфиденциальности, целостности, доступности, аутентичности и отказоустойчивости) с целью обеспечения непрерывности бизнеса, минимизации бизнес рисков, максимизации прибыли на инвестированный капитал и получения дополнительных возможностей для бизнеса.

**Конфиденциальность** - Доступность информации только для пользователей, получивших доступ к определенной информации по согласованию с ее владельцем.

**Меры защиты** - меры, вводимые для обеспечения безопасности информации, такие как административные руководящие документы (приказы, положения, инструкции), аппаратные устройства или дополнительные программы, гарантирующие целостность,



доступность и конфиденциальность данных, которые должны быть достаточно полными, точными, и своевременными, чтобы удовлетворять потребности Компании.

**Политика информационной безопасности** - совокупность правил, определяющих и ограничивающих виды деятельности объектов и участников системы информационной безопасности.

**Пользователь (информационного ресурса)** - Должностное лицо, наделенное в заявительном порядке, правами пользования и ответственностью в отношении информационного ресурса в полном или ограниченном объеме.

**Функциональное руководство** – руководящие служащие Компании, несущие ответственность согласно функциональным обязанностям в рамках своего направления внутри ООО «Эн+ Диджитал»;

**Руководитель аварийного планирования** – должностное лицо, ответственное за обеспечение безопасности жизненно важной для Компании информации и предоставление гарантий непрерывности оказания наиболее важных сервисных услуг.

## 4. Общие положения

4.1. Настоящий документ представляет собой план обеспечения непрерывности бизнеса (далее, План). Настоящий План определяет основные меры, методы и средства сохранения (поддержания) работоспособности КИВС при возникновении различных аварийных ситуаций, а также порядок работ по восстановлению процессов обработки информации в случае нарушения работоспособности КИВС и ее основных компонентов. Кроме того, План описывает действия различных категорий работников в аварийных ситуациях по ликвидации их последствий и минимизации наносимого ущерба.

4.2. Серверные комнаты – основное место расположения компонентов КИВС. Любая угроза, возникающая внутри серверной или вблизи нее, может оказать воздействие на поток жизненно важной информации через этот узел. Работа серверных комнат может быть внезапно прервана, причем такими событиями, которые сложно контролировать. Это могут быть аварии, вызываемые людьми, механическими системами, электронными системами или природными катастрофами.

4.3. План предполагает, что катастрофа нанесла серьезные повреждения одной или нескольким серверным комнатам и вынудила возобновить работу в полном объеме в оставшихся серверных комнатах либо на РВЦ. Все приложения, даже те, которые не являются очень важными, будут временно работать на резервной системе. Одновременно с работой на резервной системе ведется воссоздание основных или запасных серверных и планирование окончательного перемещения работы. Несмотря на то, что План разработан для случая серьезной катастрофы, он может быть, по решению руководства Компании, использоваться для ликвидации последствий менее опасных аварий.

4.4. Важная часть первоначальной работы по запуску информационных систем из проблемных серверных комнат это - как можно более быстрый запуск в работу наиболее критичных систем. Работа продолжается до тех пор, пока не будет, согласно плану, достигнуто полное восстановление.

## 5. Цели и задачи

5.1. Основное назначение плана обеспечения непрерывности бизнеса - это защита информационных ресурсов Компании, обеспечение безопасности жизненно важной для Компании информации и предоставление гарантий непрерывности оказания наиболее важных сервисных услуг.

5.2. Аварийная ситуация (авария) может быть определена как некоторое



произошедшее событие, которое вызывает значительные повреждения средств и систем Компании. Главное назначение Плана - свести к минимуму воздействие аварии на бизнес-процессы. План предусматривает серьезные аварии, которые вынуждают покидать основные серверные помещения и переходить на резервные.

5.3. В Плане указываются основные подходы, общие предпосылки и последовательность действий, которых необходимо придерживаться. Он обрисовывает меры подготовки, предпринимаемые до аварии и экстренные действия, которые надо выполнить сразу после нее. План является путеводителем от аварии до полного восстановления. Для того чтобы свести потери к минимуму, должно быть обеспечено восстановление производственной загрузки всех наиболее важных систем в течение суток.

5.4. План построен на концепции рабочих групп, что обеспечивает эффективность процесса восстановления. Каждая группа имеет определенные обязанности и несет ответственность после того, как было принято решение подключить ее к определенному варианту восстановительных работ. Руководители групп и их заместители набираются из ведущих сотрудников Компании.

## **6. Основные требования**

6.1. В Плане устанавливается последовательность действий рабочих групп по обнаружению аварийных ситуаций, первоначальным ответным действиям, запуску компонентов КИВС в незатронутых аварией серверных помещениях, переносу процесса обработки информации на РВЦ, восстановлению и переводу системы в штатный режим функционирования.

6.2. В случае аварийных ситуаций оперативное восстановление программ и данных в случае их уничтожения или порчи обеспечивается резервным копированием и внешним (по отношению к основным компонентам КИВС) хранением копий, а также использованием резервных (дублирующих) аппаратных средств (ресурсов).

6.3. Стратегия проведения резервного копирования и восстановления информации в КИВС, порядок проведения данных работ, необходимые действия работников по созданию, хранению и использованию резервных копий программ и данных отражены в действующих нормативно-распорядительных документах по обеспечению информационной безопасности – СТП 007-2018 «Система резервного копирования и восстановления информационных ресурсов КИВС».

6.4. Перевод процесса обработки информации в РВЦ производится по распоряжению руководства Компании на основании доклада Руководителя аварийного планирования. После завершения перевода процесса обработки информации в РВЦ Руководитель аварийного планирования докладывает руководству Компании о восстановлении работоспособности КИВС.

6.5. Ликвидация последствий аварийной ситуации подразумевает по возможности наиболее полное восстановление программных, аппаратных, информационных и других поврежденных компонентов системы. Для восстановления используются средства, перечисленные в СТП 007-2018 «Система резервного копирования и восстановления информационных ресурсов КИВС». После ликвидации последствий аварийной ситуации Руководитель аварийного планирования докладывает руководству Компании о восстановлении работоспособности КИВС в штатном режиме.

6.6. Каждая аварийная ситуация должна анализироваться в соответствии с принятой политикой информационной безопасности. По результатам этого анализа должны при необходимости выработываться предложения по изменению полномочий работников, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т.п.



6.7. В случае возникновения аварийной ситуации должно производиться расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

6.8. Если причиной аварийной ситуации явились недостаточность меры защиты и контроля, а ущерб для бизнеса Компании превысил определенный уровень, то такая ситуация является основанием для пересмотра или коррекции политики информационной безопасности и настоящего Плана.

## **7. Рабочая группа по ликвидации последствий аварии.**

7.1. Приказом ООО «Эн+ Диджитал» определяются функциональные обязанности и ответственность Руководителя аварийного планирования и руководителей рабочих групп, а также состав рабочих групп и их действия по предварительному планированию и ликвидации последствий аварии.

### **7.2. Руководитель аварийного планирования**

#### **7.2.1. Предварительное планирование:**

- Контроль за актуальностью Плана. Внесение в План уточнений и корректировок.
- Планирование тестовых проверок, подготовка Программы тестирования плана, регистрация их результатов в виде Протоколов тестирования и подготовка Отчета для руководства Компании по результатам тестирования Плана;
- Разбор результатов тестирования Плана совместно с начальниками рабочих групп;
- Доведение сведений о последних событиях и технологиях в области обеспечения непрерывности бизнеса до сотрудников Компании;
- Распространение Плана среди руководителей рабочих групп и контроль их осведомленности;
- Руководство в аварийных ситуациях, утверждение аварийных процедур;
- Доведение до Руководства ООО «Эн+ Диджитал» сведений по вопросам безопасности и ликвидации аварий;

#### **7.2.2. Действия по ликвидации аварийной ситуации:**

- Координация всех действий согласно настоящему плану, в составе группы руководства в аварийной ситуации.

### **7.3. Группа руководства в аварийной ситуации**

#### **7.3.1. Общие задачи:**

- Руководство первоначальными ответными действиями в аварийной ситуации и удостоверение, что жизни людей и собственность Компании защищены;
- Оценка ущерба;
- Определение варианта плана действий в критической ситуации;
- Уведомление функционального руководства;
- Вызов руководителей рабочих групп и начало выполнения аварийных процедур.

#### **7.3.2. Предварительное планирование:**

- Проведение ежеквартальных совещаний о текущем состоянии Плана;

#### **7.3.3. Ликвидация аварийной ситуации:**

- Создание Центра управления, для обеспечения единого руководства действиями во время аварийной ситуации;
- Сообщение в РВЦ что он будет задействован;
- Информирование функционального руководства о состоянии дел;
- Оповещение пользователей КИВС о состоянии серверных комнат;
- Обращение за профессиональной помощью к аварийным службам, поставщикам оборудования и ПО;
- Контроль процедуры перевода процесса обработки информации из ОВЦ в РВЦ.

**7.4. Группа восстановления сетевой инфраструктуры****7.4.1. Общие задачи:**

- Инсталляция прикладных систем, допускающих восстановление минимально-необходимого набора операций и коммуникаций;
- Полное восстановление баз данных;
- Организация сетевого взаимодействия;
- Восстановление функций аппаратных средств и другого оборудования КИВС или оперативная замена дефектных узлов резервными в случае отказов;
- Подготовка и оперативное включение резервных аппаратных средств и другого оборудования в случае аварийной ситуации;

**7.4.2. Предварительное планирование:**

- Обеспечение резервирования операционных систем, компьютерного и сетевого оборудования;
- Реализация процедуры резервного копирования данных на магнитные ленты, хранимые вне серверных комнат, в порядке, определенном СТП 007-2018 «Система резервного копирования и восстановления информационных ресурсов КИВС»;
- Поддержка аппаратных средств и другого оборудования КИВС, включая резервное, в рабочем состоянии и их периодическая проверка.

**7.4.3. Действия по ликвидации аварийной ситуации:**

- Установка требуемой операционной системы и других управляющих систем;
- Восстановление прикладных систем в порядке приоритетов, используя резервные магнитные ленты и проверяя непрерывность восстановления;
- Организация взаимодействия с работниками резервного центра и поставщика;
- Определение повреждения в сетях связи и обеспечение замены неисправного оборудования;
- Восстановление полного сервиса и других необходимых средств связи, совместно с телефонной компанией;
- Оповещение пользователей о задержке в предоставлении услуг;
- Восстановление баз данных с магнитных лент;
- Проверка правильности восстановления и целостности баз данных.

**7.5. Группа восстановления программных проектов.****7.5.1. Общие задачи:**

- Восстановление производственных систем и запуск процессов;
- Проверка правильности восстановления производственных систем;

**7.5.2. Предварительное планирование:**

- Контроль полноты и правильности восстановления прикладных систем и баз данных;
- Ведение реестра прикладных систем, пользователей и обязанностей работников группы поддержки программных средств КИВС;
- Определение приоритетов и процедуры восстановления прикладных систем и баз данных.

**7.5.3. Действия по ликвидации последствий аварии.**

- Приступить к восстановлению приложений и баз данных на резервной системе в соответствии с процедурой восстановления данных совместно с группой восстановления сетевой инфраструктуры;
- Проверка правильности функционирования и работоспособности приложений и процессов;
- Проверка полноты и целостности восстанавливаемой информации и баз данных;
- Наблюдение за работой наиболее важных приложений на резервной системе.



## **8. Определение приоритетов для прикладных систем**

8.1. Главная задача Плана состоит в том, чтобы обеспечить быстрое восстановление работоспособности наиболее важных прикладных систем после того, как пожар, природные катастрофы, сбои в энергоснабжении или другие причины вызывают серьезную аварию или нарушения в их нормальной работе.

8.2. Продолжение функционирования большей части всех программных систем Компании сразу после аварии вряд ли осуществимо по техническим, экономическим и организационным причинам. Но это редко необходимо, поскольку значимость систем неодинакова. Нужно осуществить анализ относительной ценности различных функций.

8.3. Для целей планирования необходимо определить два ключевых положения, для которых жизненно необходимо функционирование после аварии и какие из наиболее важных приложений потребуют неотложного внимания сразу после начала действий по ликвидации последствий аварии.

8.4. Для оценки критичности прикладных систем используются семь показателей, позволяющие установить степень уязвимости приложения к падению производительности ИТ-инфраструктуры после аварии, а также ограничения, которые могут возникнуть при восстановлении приложения:

- Допустимое время, которое может пройти перед тем, как приложение заработает после аварии;
- Особые ресурсы, которые необходимы в случае, если приложение будет восстанавливаться;
- Способность приложения переносить смену компьютера в процессе восстановления;
- Опыт сотрудников в тестировании процесса восстановления;
- Предельные значения потерь, на которые можно пойти, если восстановление приложения задерживается или невозможно;
- Структурные или функциональные ошибки, которые могут присутствовать в приложении;
- Требования к структуре или функционированию.

## **9. Средства обеспечения непрерывной работы и восстановления**

9.1. Для обеспечения работоспособности КИВС в случае выхода из строя всех или отдельных аппаратных средств из ее состава в результате возникновения аварийной ситуации предназначены резервные аппаратные средства. Количество резервных аппаратных средств и их характеристики должны обеспечивать выполнение основных задач системы.

9.2. Необходимо производить дополнительное резервирование ряда критически важных средств основного вычислительного центра.

9.3. Последствия некоторых аварийных ситуаций с высшей степенью угрозы безопасности КИВС могут быть преодолены только при использовании РВЦ, который должен обеспечивать возможность оперативного перевода на него процесса обработки информации в КИВС в случае выхода из строя ОВЦ, обеспечения работы КИВС в штатном режиме на время замены или ремонта вышедшего из строя оборудования из состава ОВЦ.

9.4. Полностью укомплектованные резервные системы, на которых было проведено тестирование операционной системы и приложений, служат страховкой на случай аварии.

9.5. Основными средствами обеспечения непрерывной работы и восстановления КИВС являются средства дублирования ресурсов КИВС и резервного копирования.

9.6. Резервированию подлежат как КИВС в целом, так и ее отдельные компоненты (серверы, внешние носители информации, оборудование в составе ЛВС и т.д.).



## **10. Резервный вычислительный центр**

10.1. РВЦ должен иметь возможность находиться в состоянии «горячего» резерва;

10.2. Характеристики каналов связи ОВЦ и РВЦ, а также имеющиеся в составе ОВЦ и РВЦ программно-аппаратные средства и персонал КИВС должны в случае аварийных ситуаций с высшей степенью угрозы безопасности КИВС обеспечивать возможность оперативного перевода процесса обработки информации из ОВЦ в РВЦ в течение часа.

10.3. В РВЦ должен быть развернут тот же состав оборудования и те же версии основного и дополнительного программного обеспечения, что и в основном вычислительном центре КИВС;

10.4. РВЦ должен быть соединен основными и резервными каналами связи с ОВЦ. Данные каналы должны быть защищены от несанкционированного доступа с помощью используемых в Компании штатных средств защиты;

10.5. РВЦ должен располагаться в отдельном от ОВЦ здании, находящемся на охраняемой территории;

10.6. Требования к помещениям для размещения РВЦ (требования по электропитанию, системам кондиционирования и другим системам жизнеобеспечения) должны соответствовать требованиям к ОВЦ;

10.7. При размещении РВЦ на той же территории, что и ОВЦ его следует подключать к фидерам электропитания и внешним каналам передачи данных, отличным от использованных в ОВЦ;

10.8. Порядок доступа к программно-аппаратным средствам РВЦ должен быть аналогичен порядку, существующему для ОВЦ.

10.9. Администрирование, техническое обслуживание РВЦ, включая процедуры резервного копирования и восстановления программ и данных, осуществляется в порядке, определенном для ОВЦ, силами работников ОВЦ. Персонал РВЦ должен пройти обучение работе с КИВС, а также регулярно проходить стажировку в ОВЦ.

10.10. Персонал РВЦ должен в случае аварийной ситуации по распоряжению руководства Компании, перевести в РВЦ процесс обработки информации и обеспечивать его сопровождение вплоть до момента возвращения обработки информации в восстановленный ОВЦ.

10.11. В обязанности персонала, уполномоченного на обслуживание РВЦ, входит:

10.11.1 периодическая проверка состояния аппаратно-программных средств и другого оборудования РВЦ, поддержание их в рабочем состоянии;

10.11.2 восстановление функций аппаратных средств и другого оборудования РВЦ или оперативная замена дефектных узлов резервными, в случае отказов.

## **11. Тестирование плана**

11.1. План необходимо регулярно тестировать, чтобы он был всегда готовым для запуска в работу в случае аварии. Тестирование должно производиться на резервной системе с использованием резервных серверных или РВЦ и документироваться.

11.2. Восстановление баз данных с магнитных лент производится в соответствии с процедурой восстановления данных.

11.3. Все критичные прикладные системы должны периодически тестироваться на резервной системе. Следует подготовить план тестирования и вести протокол всех успехов и неудач.

11.4. Использование учебной аварийной ситуации позволяет лучше оценить работоспособность и эффективность Плана. Необходимо периодически проводить учения с использованием учебной аварийной ситуации и без предупреждения.

## **12. Сопровождение плана**

12.1. После того, как План введен в действие, начинается процесс его сопровождения, чтобы обеспечить актуальность и учесть все рекомендации и предложения.

12.2. Плановые изменения дополняют промежуточные изменения, вносимые в процессе развития, включая изменения адресов, изменения аппаратной части, состава прикладных систем и т.д. Рекомендуемый срок между плановыми изменениями составляет шесть месяцев.

12.3. Каждый руководитель группы аварийного восстановления отвечает за просмотр и внесение изменений в свою часть Плана по меньшей мере раз в шесть месяцев.

12.4. Данный План подлежит пересмотру в следующих случаях:

12.4.1 при изменении перечня решаемых задач, конфигурации технических и программных средств КИВС, приводящих к изменению технологии обработки информации;

12.4.2 при изменении приоритетов в значимости угроз безопасности КИВС.

12.5. Настоящий План подлежит коррекции в следующих случаях:

12.5.1 при изменении конфигурации, добавлении или удалении программных и технических средств в КИВС, не изменяющих технологию обработки информации;

12.5.2 при изменении конфигурации используемых программных и технических средств;

12.5.3 при изменении состава, обязанностей и полномочий пользователей КИВС, ее обслуживающего персонала или аудиторов безопасности.

## **13. Ответственность**

13.1. Ответственность за осуществление общего контроля выполнения правил настоящего стандарта, а также за поддержание данного документа в актуальном состоянии несут руководитель аварийного планирования.

13.2. Ответственность за реализацию сотрудниками ИТ требований настоящего стандарта, возлагается на руководителя подразделения ИТ.

13.3. Лица, нарушающие требования настоящего стандарта несут ответственность в соответствии с действующим законодательством 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 <sup>1</sup>	Срок введения изменения	Изменения внёс			Примечания
			ФИО	Подпись	Дата внесения изменения	

<sup>1</sup> Ссылка на документ, разрешающий внесение изменений и содержащий тест изменений.