

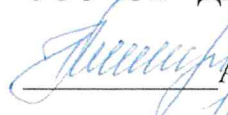
# Стандарт предприятия

---

## Система управления информационной безопасностью

Введен впервые

УТВЕРЖДАЮ  
Генеральный директор  
ООО «Эн+ Диджитал»

 А. А. Герасименко  
10.10.2018  
(дата)

Введен в действие приказом  
ООО «Эн+ Диджитал»  
от 08.10.18. № 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. Управление рисками .....	5
7. Управление непрерывностью бизнеса .....	5
8. Оповещение о нарушениях безопасности .....	6
9. Повышение осведомлённости, обучение и тренинги .....	6
10. Контроль и пересмотр .....	6
11. Ответственность .....	6
12. Список приложений .....	<b>Ошибка! Закладка не определена.</b>
Лист регистрации изменений .....	8
Приложение 1 .....	9

## 1. Область применения

1.1. Настоящий стандарт предприятия устанавливает общие требования к процедуре управления информационной безопасностью в ООО «Эн+ Диджитал» (далее Компания).

1.2. Настоящий стандарт предприятия распространяется на всех работников Компании, а также всех прочих лиц, которые обязаны выполнять требования информационной безопасности, охватываемых областью действия системы управления информационной безопасностью.

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 001-2018 «Политика в области информационной безопасности»;
- Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология – Практические правила управления информационной безопасностью»;
- Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27001-2006 – «Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Требования»;
- Международный стандарт ISO/IEC 27001:2013 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования»;
- Международный стандарт ISO/IEC 27002:2013 «Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью»;
- Гражданский кодекс РФ;
- Уголовный кодекс РФ;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера».

## 3. Сокращения и определения

3.1. В настоящем стандарте используются следующие сокращения:

**ИБ** – Информационная безопасность;

**СУИБ** – Система Управления Информационной Безопасностью.

3.2. В настоящем Стандарте используются следующие определения:

**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.

**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.

## 4. Общие положения

4.1. СУИБ должна предотвращать несанкционированный доступ к информационным ресурсам и системам Компании, включая сведения, составляющие коммерческую тайну Компании, персональные данные ее работников, а также любые другие виды закрытой информации.

4.2. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей тогда, когда они им необходимы в пределах требуемого уровня доступности ресурса. СУИБ должна осуществлять своевременное обнаружение и реагирование на угрозы, которые могут повлечь недоступность информационных ресурсов и систем.

4.3. СУИБ должна осуществлять предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

4.4. Основные процессы СУИБ это – управление рисками, управление непрерывностью бизнеса, оповещение о нарушениях безопасности, повышение осведомленности, обучение и тренинги, а также контроль и пересмотр СУИБ.

4.5. С целью поддержания СУИБ на всех уровнях управления Компании и согласованного принятия стратегически важных для Компании решений в области информационной безопасности в Компании образован Управляющий комитет по информационной безопасности.

4.6. Комитет возглавляет Председатель, который назначается на должность приказом Компании. Координация деятельности Управляющего комитета осуществляется секретарем.

4.7. Состав Управляющего комитета, его полномочия, цели и задачи, принципы функционирования и выполняемые функции определяются в соответствии положением об Управляющем комитете (Приложение 1).

4.8. СУИБ является механизмом, дающим возможность для использования информации, осуществления электронных операций и электронной коммерции, а также уменьшения информационных рисков до приемлемого уровня. Для координации методов управления данным механизмом в Компании определяется Подразделение ИБ.

## 5. Цели и задачи

5.1. Целью настоящего Стандарта является защита информационных ресурсов Компании от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, обеспечение непрерывности бизнеса и минимизация ущерба, наносимого бизнесу в результате осуществления инцидентов информационной безопасности и получение дополнительных возможностей для бизнеса.

5.2. Компания ставит своей целью получение и поддержание сертификации по требованиям международного стандарта ISO/IEC 27001:2013.

5.3. Требования информационной безопасности должны постоянно находиться в соответствии с бизнес целями Компании.

5.4. СУИБ должно быть обеспечено выполнение обязательств Компании в отношении информационной безопасности, включая защиту персональных данных работников и клиентов Компании, коммерческой тайны третьих лиц, а также других видов информации ограни-



ченного распространения, передаваемой на основании соглашений о конфиденциальности, заключаемых Компанией с организациями и гражданами.

5.5. Вводом в действие СУИБ должно быть обеспечено соответствие требованиям действующего в Российской Федерации законодательства в области информационной безопасности.

5.6. Документы СУИБ разрабатываются с учетом основных положений, перечень которых приведен ниже:

5.6.1 СТП 001-2018 «Политика в области информационной безопасности»;

5.6.2 Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология – Практические правила управления информационной безопасностью»;

5.6.3 Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27001-2006 – «Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Требования»;

5.6.4 Международный стандарт ISO/IEC 27001:2013 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования»;

5.6.5 Международный стандарт ISO/IEC 27002:2013 «Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью»;

5.6.6 Гражданский кодекс РФ;

5.6.7 Уголовный кодекс РФ;

5.6.8 Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

5.6.9 Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;

5.6.10 Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

5.6.11 Указ Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера».

## **6. Управление рисками**

6.1. Существующий в Компании стратегический бизнес-план и система управления рисками предусматривают идентификацию, оценку и контроль информационных рисков путем создания и сопровождения СУИБ. Результаты оценки рисков, заявление о применимости, план обработки рисков и политика управления рисками определяют каким образом в Компании осуществляется управление рисками информационной безопасности.

6.2. Подразделение ИБ несет ответственность за разработку и реализацию плана обработки рисков, контроль его выполнения и поддержание в актуальном состоянии.

## **7. Управление непрерывностью бизнеса**

7.1. В Компании разрабатывается и поддерживается управляемый и документированный процесс обеспечения непрерывности бизнеса, учитывающий требования информационной безопасности, и служащий для того, чтобы препятствовать прерываниям хозяйственной деятельности и защищать критические важные бизнес процессы от влияния крупных сбоев или аварий и обеспечивать их своевременное восстановление.

7.2. Планы обеспечения непрерывности бизнеса определяют общую систему мер, ответственность, необходимые требования и условия для предотвращения прерываний критически важных бизнес процессов, обеспечения требуемого уровня доступности информационных ресурсов, сервисов и инфраструктуры, а также восстановления после аварии.

7.3. Последовательность действий и способы взаимодействия персонала в критической ситуации определяются разрабатываемыми в Компании аварийными процедурами.

## **8. Оповещение о нарушениях безопасности**

8.1. Работники Компании обязаны информировать о ставших им известными фактах нарушения положений настоящего Стандарта и инцидентах информационной безопасности своего непосредственного руководителя и Подразделение ИБ.

8.2. Подразделение ИБ обязано инициировать и проводить служебные расследования по факту нарушений и инцидентов информационной безопасности, и докладывать о результатах расследований руководству Компании.

## **9. Повышение осведомлённости, обучение и тренинги**

9.1. Все работники Компании должны пройти соответствующее обучение с целью повышения осведомленности в вопросах информационной безопасности.

9.2. Работники, обеспечивающие безопасность в информационных системах, специалисты по безопасности и технический персонал Компании должны проходить специализированное обучение и практические тренинги по информационной безопасности.

## **10. Контроль и пересмотр**

10.1. СУИБ должна систематически пересматриваться и совершенствоваться.

10.2. Основными механизмами для пересмотра и совершенствования СУИБ являются внутренние и внешние аудиты безопасности, а также анализ СУИБ руководством Компании в сочетании с использованием превентивных и корректирующих мер.

10.3. Настоящий Стандарт должен пересматриваться на ежегодной основе, а также в случае любых изменений результатов оценки рисков или плана обработки рисков.

## **11. Ответственность**

11.1. Ответственность за осуществление общего контроля выполнения правил настоящего Стандарта, предоставление рекомендаций по их выполнению, а также за поддержание данного документа в актуальном состоянии несет руководитель Менеджер ИБ.

**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 внес			Примечания
			ФИО	Подпись	Дата внесения изменения	

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



## Приложение 1

**Положение о комитете по управлению информационной безопасностью Компании****1. Общие положения**

1.1. Положение о Комитете по управлению информационной безопасностью (далее - Положение) разработано для организации работы Комитета по управлению информационной безопасностью (далее - Комитет). Положение устанавливает основные цели, задачи, функции ответственность и права Комитета.

1.2. Свою деятельность Комитет осуществляет в соответствии с действующим законодательством Российской Федерации в сфере информационной безопасности, Уставом Компании, данным Положением, решениями Совета директоров и Правления.

1.3. Комитет является постоянно действующим коллегиальным органом и элементом Системы управления информационной безопасности (СУИБ) Компании.

1.4. Комитет координирует совместные действия руководителей Компании, основных структурных подразделений и представителей защиты ресурсов, Подразделения ИБ, ИТ службы.

**2. Цели и задачи Комитета****2.1. Цели Комитета:**

2.1.1. Управление информационной безопасностью в Компании путем координации совместных действий руководителей Компании, основных структурных подразделений и представителей защиты ресурсов, Подразделения ИБ, ИТ службы.

2.1.2. Разработка и принятие решений в области информационной безопасности.

**2.2. Задачи Комитета:**

2.1.3. Обеспечение безопасной работы работников Компании в автоматизированных и информационных системах Компании и предупреждение нарушений в сфере информационных технологий.

2.1.4. Работа над совершенствованием системы управления Компании, позволяющей наиболее эффективно использовать потенциал в области информационной безопасности.

2.1.5. Согласование конкретных функций и обязанностей в области информационной безопасности в рамках всей Компании.

2.1.6. Согласование конкретных методики и процедуры информационной безопасности, например, таких как оценка рисков, классификация информации с точки зрения требований безопасности.

2.1.7. Согласование и обеспечение поддержки инициатив и проектов в области информационной безопасности в рамках всей Компании, например, таких как программа повышения осведомленности работников в области безопасности.

2.1.8. Обеспечение включения требований безопасности во все проекты, связанные с обработкой и использованием информации в автоматизированных и информационных системах.

2.1.9. Оценка адекватности и координация внедрения конкретных мероприятий по управлению информационной безопасностью для новых систем или услуг.

**3. Функции Комитета**

3.1. Согласование и пересмотр политики информационной безопасности и соответствующих обязанностей по ее выполнению.

3.2. Отслеживание существенных изменений в воздействиях основных угроз информационным активам.

- 3.3. Анализ и подготовка рекомендаций (мониторинг) по актам служебного расследования инцидентов или аудиторских проверок нарушения информационной безопасности.
- 3.4. Согласование основных проектов в области информационной безопасности.
- 3.5. Разработка на основе предложений членов Комитета программы совместных действий руководителей Компании, работников защиты ресурсов, Подразделения ИБ и (или) иных уполномоченных работников по обеспечению требований информационной безопасности.
- 3.6. Внедрение стандартов информационной безопасности, рекомендуемых к принятию и исполнению контролирующими организациями.
- 3.7. Подготовка предложений руководству Компании по решению проблем информационной безопасности на основе анализа текущего состояния.

#### **4. Права Комитета**

- 4.1. Содействие во внедрении более совершенных технологий, новой техники, автоматизации с целью повышения качества обслуживания пользователей и оптимизации существующих технологий.
- 4.2. Рассмотрение проектов внутренних документов по информационной безопасности и подготовка предложений по ним руководству Компании.
- 4.3. По заданию руководства Компании, Комитет может решать и другие задачи, не отраженные в настоящем Положении.

#### **5. Организация Комитета**

- 5.1. Комитет возглавляет Председатель, который назначается на должность приказом Компании.
- 5.2. Председатель Комитета:
- 5.2.1 руководит деятельностью Комитета, организует решение стоящих перед ним задач, отчитывается за проделанную работу перед генеральным директором;
- 5.2.2 вносит руководству Компании предложения, относящиеся к деятельности Комитета;
- 5.3. В состав Комитета входят представители: основных структурных подразделений, защиты ресурсов, Подразделения ИБ, ИТ службы.
- 5.4. Представитель Подразделения ИБ является секретарем Комитета.

#### **6. Порядок работы Комитета**

- 6.1. Комитет осуществляет свою деятельность в соответствии с настоящим положением.
- 6.2. Повестка дня, время и место проведения заседания доводятся Председателем Комитета до постоянных членов не менее чем за три рабочих дня до заседания.
- 6.3. В случае созыва внеочередного заседания Комитета повестка дня согласовывается инициатором проведения заседания с Председателем.
- 6.4. Решения на заседаниях Комитета принимаются простым большинством голосов присутствующих на заседании членов Комитета. При равенстве голосов, голос Председателя комитета является решающим. Каждый член Комитета обладает одним голосом.
- 6.5. Документы, рассматриваемые на заседаниях, утверждаются Комитетом путем голосования и передаются для рассмотрения в соответствии с порядком утверждения документов, разработанных в Компании. Документ считается утвержденным Комитетом, если за него проголосовало не менее половины присутствующих на заседании постоянных членов Комитета.
- 6.6. Согласование документов, проектов внедрения, требующих выполнение правил ИБ и касающиеся деятельности Комитета, выполняется в заочном режиме. На листе согласо-



вания документа или в его визовой части вносятся все должностные лица Комитета. Документ с листом согласования направляются членам Комитета с указанием срока, отведенного для голосования (не менее 2 рабочих дней).

6.7. Все материалы, разработанные и утвержденные Комитетом для использования работниками Компании, но не требующие утверждения руководством, должны доводиться до работников Компании.

6.8. По решению Комитета, его членам, экспертам или рабочим группам может поручаться разработка проектов документов для рассмотрения на Комитете.

6.9. На заседаниях Комитета ведется протокол заседания. Протоколы должны храниться в течение 5 лет у секретаря и быть доступными для ознакомления всем руководителям подразделений Компании.