

	Политика Системы управления информационной безопасностью ООО «Открытая мобильная платформа»	
Редакция: 1.2/2019	Утверждено и введено в действие приказом от «12» июля 2019 г. № 12-од	Стр. 1 из 12

**Общество с ограниченной ответственностью  
«Открытая мобильная платформа»  
(ООО «Открытая мобильная платформа»)**

ИНН 1615012605 КПП 161501001 ОГРН 1161690087020 ОКПО 01852515

УТВЕРЖДЕНО  
Приказом генерального директора  
ООО «Открытая мобильная  
платформа»  
от «12» июля 2019 г. № 12-од

**Политика**

**Системы управления информационной безопасностью  
ООО «Открытая мобильная платформа»**

г. Иннополис, 2019 г.

### Информация о документе

<b>Процесс 1 уровня</b>	С 9 Управление безопасностью и непрерывностью
<b>Процесс 2 уровня</b>	С 9.1 Система управления информационной безопасностью
<b>Автор</b>	Начальник отдела информационной безопасности и непрерывности Руднев С.А.
<b>Статус</b>	<i>Проект</i> <i>Утвержден приказом от 12.07.2019 № 12-од (реквизиты приказа);</i> <i>Отменен (реквизиты приказа)</i>
<b>Подразделение владельца документа</b>	Отдел информационной безопасности и непрерывности

Настоящий документ и его содержание являются собственностью ООО «Открытая мобильная платформа». Настоящий документ содержит конфиденциальную информацию. Воспроизведение, распространение, использование или передача этого документа или любой его части без специального разрешения строго запрещены. Правонарушители будут считаться ответственными за возмещение возможных, в связи с этим правонарушением убытков. Все права защищены.

### Кодификация документа

Организация-автор	Направление деятельности/ бизнес-процесс	Тип документа	Порядковый номер	Версия	Дата
ОМП	УК.С9	ПЛ	01	2	15.06.2018

### История изменений

№ документа (редакции)	Дата внесения изменения	Автор документа/изменения (ФИО, подразделение)	Содержание изменения
1.0		Руднев С. А., начальник отдела информационной безопасности и непрерывности	Разработка документа
0.2.	12.07.2019	Руднев С. А., начальник отдела информационной безопасности и непрерывности	Пересмотр целей политики СУИБ

### Лист согласования (если требуется)

№	И.О. Фамилия	Должность	Подпись	Дата

## СОДЕРЖАНИЕ

1. Назначение .....	4
2. Общие положения.....	4
2.1 Область применения.....	4
2.2 Нормативные ссылки.....	4
2.3 Термины, определения и сокращения.....	4
3. Основные положения .....	5
4. Область деятельности СУИБ.....	5
5. Цели и задачи системы управления ИБ.....	6
6. Принципы СУИБ .....	7
7. Стратегическое управление СУИБ .....	7
8. Определение ролей и ответственности.....	8
9. Управление рисками.....	8
10. Управление документацией СУИБ.....	8
11. Обучение персонала .....	8
12. Организация работы со сторонними организациями.....	9
13. Внутренние аудиты ИБ .....	9
14. Мониторинг, анализ эффективности и совершенствование процессов СУИБ .....	10
15. Соответствие требованиям законодательства .....	10
15.1 Защита права интеллектуальной собственности .....	10
15.2 Защита персональных данных.....	10
16. Порядок внесения изменений.....	10
17. Контроль за исполнением Политики.....	11
17.1 Контроль выполнения требований Политики .....	11
18. Ответственность работников.....	11
19. Хранение и архивирование.....	11
20. Рассылка и актуализация .....	11

## 1. Назначение

- 1.1 Настоящая Политика Системы управления информационной безопасностью (далее по тексту — Политика) устанавливает общие требования к процессам и системе управления информационной безопасностью (далее по тексту — СУИБ) ООО «Открытая мобильная платформа» (далее по тексту — Компания) в целом, а также определяет основные принципы и подходы к обеспечению информационной безопасности (далее по тексту — ИБ).

## 2. Общие положения

### 2.1 Область применения

Требования настоящей Политики являются обязательными для исполнения работниками всех структурных подразделений Компании, подрядчиков и контрагентов, допущенных к активам Компании.

### 2.2 Нормативные ссылки

В настоящей Политике использованы ссылки на следующие нормативные документы:

- 2.2.1 ISO/IEC 27001:2013 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- 2.2.2 ГОСТ Р ИСЭ/МЭК 27000-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»;
- 2.2.3 ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;
- 2.2.4 И-30.1-2018 Инструкция по управлению внутренней нормативной документацией ООО «Открытая мобильная платформа»;
- 2.2.5 И-25.1-2018 Инструкция по делопроизводству в ООО «Открытая мобильная платформа»;
- 2.2.6 И-27.1-2018 Инструкция по управлению записями в ООО «Открытая мобильная платформа».

### 2.3 Термины, определения и сокращения

- 2.3.1 В настоящей Политике использованы следующие термины, определения и сокращения:

Термин/сокращение	Определение
<b>Актив</b>	Все, что имеет ценность для Компании. К активам относятся: информационные системы, информация, программное обеспечение, оборудование, сервисы, работники Компании и т. д.
<b>Владелец актива</b>	Работник Компании, уполномоченный управлять созданием, разработкой, поддержанием, использованием и защитой активов
<b>Владелец процесса</b>	Владелец соответствующего бизнес-процесса, предусмотренного моделью процессов Общества
<b>Доступность</b>	Свойство быть доступным и готовым к использованию по запросу авторизованного субъекта
<b>Информация</b>	Знания или данные, которые имеют значение для Компании
<b>Информационная безопасность</b>	Сохранение конфиденциальности, целостности и доступности информации

<b>Термин/сокращение</b>	<b>Определение</b>
<b>Комитет по ИБ</b>	Коллегиальный орган, созданный в целях координации и контроля за организацией работ по обеспечению информационной безопасности в Компании, а также для принятия стратегических решений по развитию информационной безопасности в Компании.
<b>Компания</b>	ООО «Открытая мобильная платформа»
<b>Конфиденциальность</b>	Свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов
<b>Область деятельности СУИБ</b>	Область применения и границы СУИБ в контексте бизнес-процессов, подразделений Компании, территориальных площадок, ресурсов и применяемых технологий
<b>Система управления информационной безопасностью</b>	Часть общей системы управления Компании, предназначенная для разработки, внедрения, применения, мониторинга, анализа, поддержания и улучшения процессов обеспечения ИБ Компании. СУИБ включает организационную структуру, политику, планирование, обязанности участников процессов СУИБ, процессы и ресурсы в области ИБ
<b>Целостность</b>	Свойство сохранения правильности и полноты активов
<b>ИБ</b>	Информационная безопасность
<b>ОД</b>	Область деятельности
<b>ПДн</b>	Персональные данные
<b>СУИБ</b>	Система управления информационной безопасностью

### **3. Основные положения**

- 3.1 Одним из важнейших активов Компании является информация, значимая для его деятельности, в том числе используемая в ходе взаимодействия с клиентами и партнерами.
- 3.2 Нарушение применимых требований ИБ может привести к серьезным последствиям, таким как финансовые потери, правовые санкции, ущерб репутации Компании, в том числе потеря доверия со стороны клиентов и партнеров, снижение конкурентоспособности на международных рынках.
- 3.3 Надлежащий уровень ИБ в Компании обеспечивается в соответствии с требованиями бизнеса, требованиями законодательства и регуляторов в части ИБ путем внедрения и непрерывного совершенствования СУИБ на основе международных стандартов и практик.

### **4. Область деятельности СУИБ**

- 4.1 Для эффективной реализации процессов обеспечения ИБ в Компании внедряется СУИБ, соответствующая требованиям международного стандарта ISO/IEC 27001:2013 [2.2.1]. Для обеспечения реализации процессов жизненного цикла безопасной разработки программного обеспечения в Компании реализуются требования положений ГОСТ Р 56939-2016 [2.2.3].
- 4.2 СУИБ должна, в первую очередь, распространяться на ключевой бизнес-процесс,

безопасность и непрерывность которого важно обеспечить для стабильного функционирования всей Компании.

- 4.3 СУИБ внедряется на один из ключевых бизнес-процессов Компании — «Поддержание жизненного цикла безопасной разработки программного обеспечения». Описание данного бизнес-процесса, входящих в него подразделений и активов, а также обоснование выбора, данного бизнес-процесса в качестве области деятельности СУИБ будут приведены в документе «Область деятельности системы управления информационной безопасностью».

## 5. Цели и задачи системы управления ИБ

- 5.1 Перечень активов Компании регулярно пересматривается и актуализируется в соответствии с процессом анализа рисков ИБ.
- 5.2 Основная цель СУИБ — создание и постоянное поддержание в Компании условий, при которых риски, связанные с обеспечением безопасности активов Компании, постоянно контролируются и находятся на приемлемом уровне.
- 5.3 Достижение данной цели позволяет:
- защитить активы Компании от всех видов угроз (внешних и внутренних, умышленных и непреднамеренных);
  - обеспечить непрерывность бизнеса;
  - обеспечить соответствие Компании требованиям действующего законодательства и регуляторов в области ИБ;
  - обеспечить соответствие процессов обеспечения ИБ бизнес-требованиям Компании;
  - минимизировать ущерб, наносимый бизнесу в результате возникновения инцидентов ИБ;
  - увеличить прибыли на инвестированный капитал и получить дополнительные возможности для бизнеса;
  - обеспечить доверие клиентов и партнеров Компании.
- 5.4 Вышеописанная цель достигается решением следующих задач:
- инвентаризация активов Компании и регулярное проведение оценки рисков ИБ;
  - применение обоснованных, экономически эффективных организационных и технических мер по обеспечению ИБ;
  - реализация требований по разработке безопасного программного обеспечения и созданию жизненного цикла разработки программного обеспечения;
  - выявление применимых требований действующего законодательства и регуляторов в области ИБ, достижение соответствия этим требованиям;
  - установление ответственности работников по вопросам обеспечения ИБ, обучение и повышение их осведомленности в части ИБ;
  - регулярная оценка соответствия СУИБ применимым внутренним и внешним требованиям посредством проведения внутренних аудитов СУИБ, мониторинга эффективности процессов СУИБ, анализа СУИБ руководством Компании;
  - внедрение корректирующих действий в случае выявления отклонений или несоответствий в работе СУИБ внутренним и внешним требованиям;

- подтверждение соответствия СУИБ Компании требованиям международного стандарта ISO/IEC 27001:2013 [2.2.1].

## 6. Принципы СУИБ

В процессе обеспечения ИБ Компании должно руководствоваться принципами, приведенными ниже:

**Законность.** При обеспечении ИБ выполняются требования применимого законодательства, а также действующие нормативные требования государственных регулирующих органов, в том числе, международных.

**Адекватность** существующим угрозам и экономическая обоснованность. Применяемые организационные и технические меры защиты выбираются исходя из потребностей бизнеса на основе результатов анализа и оценки рисков ИБ, в частности, анализа актуальных угроз и затрат на внедрение и сопровождение мер управления рисками. Проводится периодическая оценка эффективности используемых мер и механизмов защиты.

**Минимизация** ограничивающего влияния на бизнес-процессы. Применяемые организационные и технические меры СУИБ минимально влияют на функционирование и характеристики бизнес-процессов Компании.

**Перспективность** и ориентация на существующие российские и международные открытые стандарты. Организационные и технические меры СУИБ реализуются с учетом мировых тенденций в области ИБ. Ориентация на открытые стандарты позволяет использовать накопленный мировой опыт в области защиты информации, а также обеспечивает прозрачность процессов ИБ и простоту взаимодействия в рамках задач по обеспечению ИБ.

**Непрерывность функционирования.** Обеспечиваются отказоустойчивость, надежность, доступность и корректность функционирования организационных и технических мер СУИБ.

**Непрерывность совершенствования.** Для успешного противодействия угрозам ИБ в условиях постоянно меняющегося внешнего и внутреннего окружения реализуется непрерывный цикл развития и совершенствования СУИБ.

**Персональная ответственность.** Каждый работник Компании несет персональную ответственность за выполнение функций и требований, возложенных на него в рамках функционирования СУИБ.

**Контроль.** Осуществляется постоянный контроль выполнения работниками Компании требований в области ИБ.

## 7. Стратегическое управление СУИБ

- 7.1 Деятельность по обеспечению ИБ в Компании должна планироваться ежегодно на уровне высшего руководства. Ресурсы на поддержку и модернизацию СУИБ должны регулярно выделяться высшим руководством.
- 7.2 В целях координации действий структурных подразделений Компании по обеспечению ИБ должен быть сформирован коллегиальный орган, выполняющий функции контроля, анализа и совершенствования СУИБ — Комитет по ИБ.
- 7.3 Ответственность за ИБ должна быть четко определена и документирована.

## **8. Определение ролей и ответственности**

- 8.1 Для достижения заявленных целей Компании в сфере ИБ для работников и представителей сторонних организаций должна быть определены роли и ответственность.
- 8.2 Требования к порядку назначения работников на роли, зонам их ответственности должны быть детально документированы в нормативных документах Компании.

## **9. Управление рисками**

- 9.1 В соответствии с риск-ориентированным подходом, устанавливаемым настоящей Политикой, в Компании должны регулярно проводиться инвентаризация активов, категорирование информации, а также анализ и оценка рисков в соответствии с разработанной процедурой управления рисками ИБ, которая предусматривает идентификацию, анализ и оценку рисков ИБ, обработку неприемлемых рисков.
- 9.2 Результаты оценки рисков, состав применяемых в Компании мер обеспечения ИБ и планы по обработке рисков должны быть сформированы в соответствии с принятой в Компании методикой по управлению рисками ИБ.
- 9.3 Ответственность за пересмотр рисков, разработку и контроль исполнения мероприятий по минимизации рисков, утверждение критериев принятия рисков ИБ должна быть определена и документирована.

## **10. Управление документацией СУИБ**

- 10.1 Разработка, оформление, согласование, регистрация, хранение, передача и уничтожение документации, относящейся к СУИБ Компании, должны соответствовать принятым в Компании требованиям по управлению организационно-распорядительной документацией.
- 10.2 Доступ к документации, представленной как на печатных носителях, так и в электронном виде и содержащей конфиденциальную информацию, должен быть ограничен и предоставляться только тем работникам Компании, контрагентам и партнерам, которые прошли необходимые процедуры получения соответствующих прав доступа.
- 10.3 В поддержку организационно-распорядительной документации СУИБ Компании должны создаваться записи, которые являются свидетельствами выполнения процессов управления и обеспечения ИБ и результативности функционирования СУИБ Компании в целом.

## **11. Обучение персонала**

- 11.1 Работники Компании должны регулярно проходить обучение (повышение уровня знаний) в области ИБ.
- 11.2 Работники Компании, ответственные за определение и контроль требований по ИБ, должны постоянно поддерживать уровень своей компетенции, принимая участие в различных выставках, форумах и конференциях по ИБ, изучая методики, признанные лучшими мировыми практиками, а также используя источники массовой информации.
- 11.3 Должен проводиться регулярный контроль знаний работников Компании в области ИБ.



## 12. Организация работы со сторонними организациями

- 12.1 Компания в процессе своей деятельности взаимодействует со следующими сторонними организациями:
- Головная Компания ПАО «Ростелеком»;
  - партнеры;
  - заказчики (юридические лица);
  - регуляторы;
  - государственные органы;
  - поставщики товаров и услуг.
- 12.2 При заключении договоров со сторонними организациями необходимо учитывать требования ИБ обеих сторон. Согласованные требования по ИБ, касающиеся порядка обмена, обработки, хранения и распространения информации, предоставления доступа сторонних организаций к активам Компании должны быть зафиксированы в договоре и/или соглашении о конфиденциальности.
- 12.3 В договоре с контрагентами, оказывающими услуги по обеспечению физической безопасности и обслуживанию ИТ-инфраструктуры Компании, должны быть учтены требования к порядку осуществления доступа на территорию, в помещения и к активам Компании.
- 12.4 Взаимодействие с международными и российскими регуляторами, государственными органами регламентируются соответствующими федеральными законами и другими нормативно-правовыми актами Российской Федерации, применимым международным законодательством.

## 13. Внутренние аудиты ИБ

- 13.1 В Компании должны регулярно (не реже раза в год) проводиться внутренние аудиты СУИБ с целью проверки того, что процессы, процедуры и меры обеспечения ИБ:
- соответствуют требованиям нормативных документов СУИБ;
  - соответствуют требованиям ГОСТ Р 56939-2016 [2.2.3], предъявляемым к жизненному циклу безопасной разработки программного обеспечения;
  - соответствуют требованиям ISO/IEC 27001:2013 [2.2.1], а также требованиям действующего законодательства;
  - реализованы и сопровождаются в соответствии с установленными целями и задачами ИБ.
- 13.2 Критерии, область аудита, частота, методы проведения, ответственность, требования к планированию и проведению аудитов в Компании, а также к предоставлению отчетов по результатам и ведению записей должны быть определены и документированы.
- 13.3 Выбор аудиторов и проведение аудитов должны гарантировать объективность и непредвзятость процесса аудита. Аудиторы не должны проверять свою собственную работу.
- 13.4 Выявленные в ходе внутренних аудитов несоответствия и их причины должны устраняться корректирующими мероприятиями.
- 13.5 Доступ к техническим средствам проведения аудита должен быть защищен с целью

предотвращения возможного ненадлежащего использования и компрометации. Доступ к результатам аудита со стороны работников Компании и/или работников сторонних организаций должен быть ограничен.

## **14. Мониторинг, анализ эффективности и совершенствование процессов СУИБ**

- 14.1 В Компании должен проводиться регулярный мониторинг процессов СУИБ с целью:
- быстрого обнаружения ошибок, отклонений и несоответствий в результатах обработки информации, выполнении процессов обеспечения и управления ИБ, а также выявления причин этих отклонений;
  - быстрого выявления удавшихся и неудавшихся попыток нарушений и инцидентов ИБ;
  - оценки эффективности мероприятий, предпринятых для совершенствования СУИБ (путем введения специальных показателей эффективности).
- 14.2 В Компании регулярно, не менее одного раза в год, должен проводиться анализ СУИБ. При этом должны учитываться результаты проведения аудитов безопасности, статистика и дополнительная информация по произошедшим инцидентам ИБ, результаты оценки эффективности процессов ИБ, а также предложения и комментарии от всех заинтересованных сторон.
- 14.3 В Компании должна непрерывно совершенствоваться СУИБ путем применения корректирующих мер, определенных по результатам анализа СУИБ. Порядок выбора, согласования и применения корректирующих мер должен быть документирован.

## **15. Соответствие требованиям законодательства**

### **15.1 Защита права интеллектуальной собственности**

- 15.1.1 В Компании должно обеспечиваться соблюдение требований законодательства и договорных отношений в области использования материалов, охраняемых правом интеллектуальной собственности, а также в области использования коммерческого программного обеспечения.
- 15.1.2 В Компании допустимо к использованию только законно введенное в оборот и легально реализуемое программное обеспечение.

### **15.2 Защита персональных данных**

- 15.2.1 В Компании должны быть определены и реализованы требования к обработке и обеспечению безопасности персональных данных в соответствии с действующим законодательством, требованиями и рекомендациями регулирующих органов.
- 15.2.2 Требования к сбору, систематизации, уточнению, хранению, использованию, распространению, обезличиванию, блокированию и уничтожению персональных данных должны быть определены в нормативных документах Компании.

## **16. Порядок внесения изменений**

- 16.1 Ответственным за актуализацию Политики является Начальник отдела информационной безопасности и непрерывности.
- 16.2 Настоящая Политика пересматривается не реже, чем раз в три года.

16.3 Внеплановый пересмотр настоящей Политики может осуществляться также в следующих случаях:

- при существенном изменении организационной структуры Компании, структуры активов и применения новых технологий передачи, хранения и обработки информации;
- по результатам проведения проверки соответствия ИБ (аудит, оценка эффективности);
- по результатам анализа произошедших инцидентов ИБ;
- по результатам анализа рисков ИБ.

## **17. Контроль за исполнением Политики**

### **17.1 Контроль выполнения требований Политики**

17.1.1 Все работники Компании несут дисциплинарную ответственность за несоблюдение требований Политики.

17.1.2 Контроль за соблюдением требований Политики в Компании осуществляет Генеральный директор.

## **18. Ответственность работников**

18.1 В случае нарушения требований ИБ работник может быть привлечен к дисциплинарной, материальной, административной, уголовной ответственности в соответствии с законодательством Российской Федерации.

## **19. Хранение и архивирование**

19.1 Подлинник настоящей Политики во время срока действия хранится в соответствии с И-25.1-2018 Инструкцией по делопроизводству в ООО «Открытая мобильная платформа».

19.2 Актуальная электронная версия документа доступна по ссылке: [cloud.omprussia.ru/ISMS/СУИБ](http://cloud.omprussia.ru/ISMS/СУИБ).

19.3 Пользователи неконтролируемых бумажных копий документа обязаны сверять их на соответствие последнему изданию в списке утвержденных документов, размещенном на сетевом разделе: [cloud.omprussia.ru/ISMS/СУИБ](http://cloud.omprussia.ru/ISMS/СУИБ).

## **20. Рассылка и актуализация**

20.1 Периодическая проверка настоящей Политики проводится Начальником отдела информационной безопасности и непрерывности, по мере необходимости, но не реже 1 раза в 12 месяцев.

20.2 Решение об инициации процесса внесения изменений в документ принимает председатель Комитета ИБ, на основании предложений других подразделений, результатов применения документа в ООО «Открытая мобильная платформа», анализа зарегистрированных и устраненных несоответствий, а также рекомендаций внутренних или внешних аудитов.

20.3 Порядок периодической проверки и внесения изменений в документ определен в И-30.1-2018 Процедура по управлению внутренней нормативной документацией

ООО «Открытая мобильная платформа».

- 20.4 Актуальная версия утвержденного документа размещается на Интранет-портале и в Журнале регистрации и учета внутренней нормативной документации. Ответственность за размещение и поддержание в актуальном состоянии размещенных на Интранет-портале документов, а также доведение информации о месте размещения актуальных версий до всех заинтересованных подразделений несет подразделение-разработчик документа.