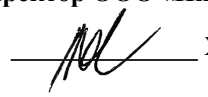
Утверждаю

Директор ООО «Интернет-Про»



Халиков А.Р.

АКТ

Оценки эффективности принимаемых мер
по обеспечению безопасности персональных данных
для 3-го уровня защищенности

г. Екатеринбург, 2025

1. ООО «Интернет-Про» проведена оценка эффективности принимаемых мер и соответствия системы защиты информационной системы «Платформа NetAngels» требованиям по обеспечению безопасности персональных данных, определенным в Приказе ФСТЭК России № 21 от 18 февраля 2013 г «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Информационная система «Платформа NetAngels» включает следующие сервисы:

— Группа услуг «Облачные VDS», включая:

Виртуальные машины

Виртуальные диски

Виртуальные сети

Бэкапы

3. Технические средства информационной системы «Платформа NetAngels» располагаются

на следующих территориальных площадках:

— Екатеринбург, проспект Космонавтов, 101

4. Оценка эффективности принимаемых мер проведена в форме приемочных испытаний системы защиты информационной системы «Платформа NetAngels».

5. По результатам проведения оценки эффективности принимаемых мер и соответствия системы защиты требованиям по обеспечению безопасности персональных данных установлено, что система защиты информационной системы «Платформа NetAngels» соответствует требованиям к составу и содержанию мер по обеспечению безопасности персональных данных для 3-го уровня защищенности (УЗ-3) персональных данных, а также обеспечивает защиту от актуальных угроз безопасности информации.

6. Результаты оценки действуют в течение 3 (трех) лет. При изменении структурно-функциональных характеристик информационной системы «Платформа NetAngels», условий ее эксплуатации, изменения требований, на соответствие которым проводилась оценка, появлении новых актуальных угроз безопасности информации проводится повторная оценка.

7. Обеспечение безопасности информации, обрабатываемой с использованием информационной системы «Платформа NetAngels» и размещаемых на ее базе информационных систем, выполнение требований законодательства – совместная ответственность ООО «Интернет-Про» и клиентов. Разграничение зон ответственности приведено в Приложении 1.

8. Перечень мер, на соответствие которым проводилась оценка, приведён в Приложении 2. Также указанное приложение содержит сведения о мерах, которые необходимо реализовать в клиентских информационных системах, размещённых на базе информационной системы «Платформа Netangels», для обеспечение безопасности персональных данных 3-го уровня защищённости (УЗ-3)

Директор ООО «Интернет-Про» 


А.Р.Халиков

Приложение 1

Разграничение зон ответственности в части обеспечения безопасности

Информационная система «Платформа NetAngels»

Информационная система «Платформа NetAngels» представляет собой распределенную вычислительную инфраструктуру, состоящую из набора инфраструктурных сервисов, предназначенную для размещения на ее базе клиентских информационных систем, в том числе информационных систем персональных данных до 3-го уровня защищенности (УЗ-3) включительно.

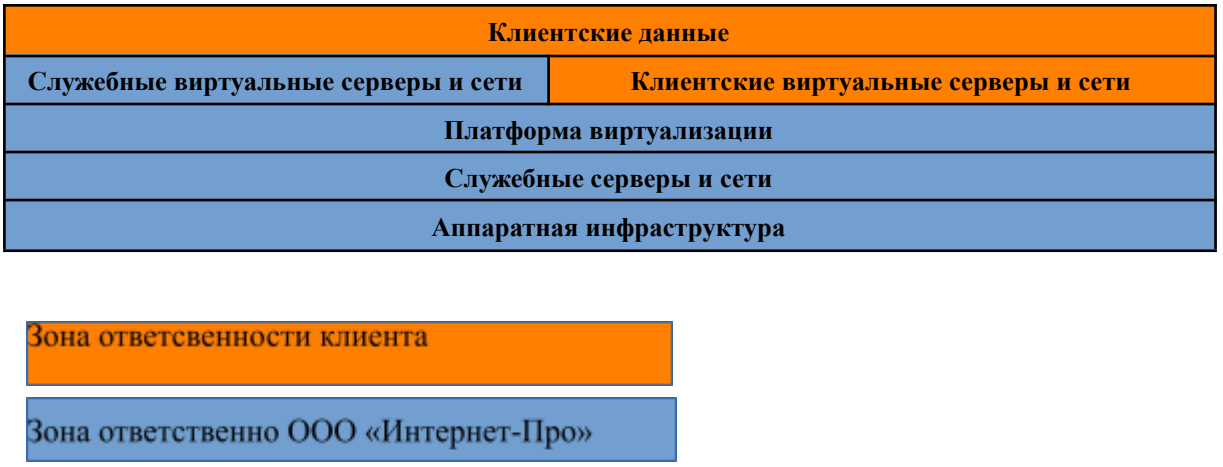
Обеспечение безопасности информации, обрабатываемой с использованием информационной системы «Платформа NetAngels» и размещаемых на ее базе информационных систем клиентов, а также выполнение требований законодательства – совместная ответственность ООО «Интернет-Про» и клиентов.

Разграничение ответственности между ООО «Интернет-Про» и клиентами при пользовании сервисами, указанными в п. 2, реализуется следующим образом:

1. ООО «Интернет-Про» в общем случае отвечает за обеспечение информационной безопасности служебной инфраструктуры информационной системы «Платформа NetAngels» - обеспечивает физическую безопасность и отказоустойчивость оборудования, сетевую безопасность служебных сетей, безопасность платформы виртуализации и служебных серверов.

2. Клиент отвечает за обеспечение информационной безопасности размещаемых на базе информационной системы «Платформа NetAngels» собственных информационных систем - обеспечивает безопасность виртуальных серверов (включая операционные системы и приложения), сетевую безопасность клиентских сетей, организует управление доступом к обрабатываемым данным.

Схематично разграничение зон ответственности между ООО «Интернет-Про» и клиентом представлено на схеме ниже:



Приложение 2

Выполнение мер по обеспечению безопасности информации

Информационная система «Платформа NetAngels»

Выполнение мер, необходимых для обеспечения безопасности персональных данных 3-го уровня защищенности (УЗ-3), а также для защиты от актуальных угроз безопасности, осуществляется за счет использования штатного функционала системного и прикладного программного обеспечения, входящего в состав информационной системы «Платформа NetAngels», а также применяемых средств защиты информации и комплекса организационных мер.

Перечень реализуемых ООО «Интернет-Про» мер, сформированный с учетом требований Приказа ФСТЭК России № 21 от 18.02.2013 и Постановления Правительства РФ от 01.11.2012 № 1119, приведен в таблице ниже. Кроме того, указанная таблица содержит перечень мер, которые необходимо реализовать в клиентских информационных системах, размещаемых на базе информационной системы «Платформа NetAngels», для обеспечения безопасности персональных данных 3-го уровня защищенности (УЗ-3).

Обозначение меры	Описание меры	Реализация ООО «Интернет-Про»	Реализация клиентом
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками	Реализуется на уровне сетевого оборудования, служебных серверов и платформы виртуализации (далее — служебная инфраструктура)	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Не применимо, т.к. внешние пользователи служебной инфраструктуры отсутствуют	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	Реализуется для служебных сетей	Необходимо реализовать для клиентских сетей
УПД.4	Разделение полномочий (ролей) пользователей,	Реализуется на уровне служебной	Необходимо реализовать на уровне

Обозначение меры	Описание меры	Реализация ООО «Интернет-Про»	Реализация клиентом
	администраторов и лиц, обеспечивающих функционирование информационной системы	инфраструктуры	клиентских виртуальных серверов и приложений
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Не применимо, т. к. технология не используется	Не применимо, т. к. технология не используется
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Не применимо, т. к. технология не используется	Не применимо, т. к. технология не используется
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или	Реализуется на уровне технических средств	Не применимо, т. к. технические средства не входят в зону ответственности клиента

Обозначение меры	Описание меры	Реализация ООО «Интернет-Про»	Реализация клиентом
	утилизации, а также контроль уничтожения (стирания) или обезличивания		
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
РСБ.7	Защита информации о событиях безопасности	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
АВЗ.1	Реализация антивирусной защиты	Реализуется на уровне служебных серверов	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Реализуется на уровне служебных серверов	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений

Обозначение меры	Описание меры	Реализация ООО «Интернет-Про»	Реализация клиентом
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	Реализуется на уровне служебной сети	Необходимо реализовать на уровне клиентских сетей
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Реализуется на уровне технических средств	Не применимо, т. к. технические средства не входят в зону ответственности клиента
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Не применимо, т. к. устройства вывода не входят в состав информационной системы	Не применимо, т. к. устройства вывода не входят в состав информационной системы
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода	Реализуется на уровне служебной сети	Необходимо реализовать на уровне клиентских виртуальных серверов и

Обозначение меры	Описание меры	Реализация ООО «Интернет-Про»	Реализация клиентом
	ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи		приложений
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Не применимо, т. к. технология не используется	Не применимо, т. к. технология не используется
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне клиентских виртуальных серверов и приложений