ООО “Энвибокс”, ИНН 5836683285
440000, г. Пенза, ул. Кураева, стр 26
support@envybox.io

Акт
оценки эффективности принимаемых мер по обеспечению безопасности персональных данных в информационной системе “Envybox”
№ 4/ОПДН от 22.05.2025

1. ООО “Энвибокс”, в лице комиссии, ответственной за оценку эффективности принимаемых мер по обеспечению безопасности персональных данных, в составе:

- председателя комиссии - генерального директора Смирнова Денис Андреевича, ответственного за организацию обработки персональных данных
- члена комиссии - специалиста службы информационной безопасности - Фомина Игоря Олеговича
- члена комиссии - директора по развитию - Молчанова Алексея Викторовича

в соответствии с требованием Федерального закона 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» провели оценку эффективности принимаемых мер и соответствия системы защиты информационной системы “Envybox”.

2. Оценка эффективности принимаемых мер проведена в форме приемочных испытаний системы защиты информационной системы «Envybox»

3. По результатам проведения оценки эффективности принимаемых мер и соответствия системы защиты требованиям по обеспечению безопасности персональных данных установлено, что система защиты информационной системы «Envybox» 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.

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

5. Перечень мер, на соотвествие которые проводилась оценка приведен в Приложение №1

Председатель Д.А. Смирнов

Член комиссии И.О. Фомин

Член комиссии А.В. Молчанов

Приложение №1

Перечень мер по обеспечению безопасности информации
информационной системы “Envybox”

Обозначение меры	Описание меры	Соответствие
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Соответствует
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Соответствует
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	Соответствует
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Соответствует
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Соответствует
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Соответствует
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Соответствует
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	Соответствует
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Соответствует

УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Соответствует
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Соответствует
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Соответствует (по запросу)
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Соответствует
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Соответствует (работники оператора) Не применимо (внешние пользователи ИС)
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Соответствует (работники оператора) Не применимо (внешние пользователи ИС)
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Соответствует (работники оператора) Не применимо (внешние пользователи ИС)
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Соответствует
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или	Соответствует

	утилизации, а также контроль уничтожения (стирания) или обезличивания	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Соответствует
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Соответствует
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Соответствует
РСБ.7	Защита информации о событиях безопасности	Соответствует
АВЗ.1	Реализация антивирусной защиты	Соответствует
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Соответствует
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Соответствует
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Соответствует
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Соответствует
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Соответствует
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Соответствует
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	Соответствует
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	Соответствует
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	Соответствует

ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	Соответствует
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	Соответствует (работники оператора) Не применимо (внешние пользователи ИС)
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Соответствует (работники оператора) Не применимо (внешние пользователи ИС)
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	Соответствует
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Соответствует (работники оператора) Не применимо (внешние пользователи ИС)
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	Соответствует
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	Соответствует
УКФ.3	Анализ потенциального воздействия	Соответствует

	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	
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	Соответствует