Заключение
о соответствии системы защиты персональных данных требованиям законодательства

ООО «Ореол Секьюрити» (Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации от 28 февраля 2020 г. №Л024-00107-00/00581776 – Приложение № 1) проведена оценка эффективности принимаемых мер и соответствия системы защиты ИСПДн ООО «Консоль.Про» (далее – Компания) требованиям по обеспечению безопасности персональных данных, установленными:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

По результатам проведенной оценки принимаемых мер установлено, что система защиты персональных данных ИСПДн «Консоль.Про» в отношении информационных систем:

- ИС «Консоль»;
- ИС «konsol.pro»;
- ИС «АРМ Пользователей»

соответствует требованиям законодательства к составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных для 3 (Третьего) уровня защищенности персональных данных.

Результаты оценки действуют в течении 3 (Трех) лет.

Перечень мер, реализованных для выполнения требований к 3 (Третьему) уровню защищенности персональных данных в ИСПДн ООО «Консоль.Про», приведен в Приложении № 2.

Дата подписания**: 12.12.2022**

_____ **В.Ю. Носаков**

м.п. **Генеральный директор ООО «Ореол Секьюрити»**

Приложение № 1

Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации от 28 февраля 2020 г. №Л024-00107-00/00581776[1]

Регистрационный номер лицензии	Л024-00107-00/00581776
Дата предоставления лицензии	28.02.2020
Срок действия лицензии	бессрочно
Полное (сокращенное) наименование лицензиата	Общество с ограниченной ответственностью «Ореол Секьюрити» (ООО «Ореол Секьюрити»)
ОГРН или ОГРИП лицензиата	1195053003276
ИНН лицензиата	5029238654
Адрес места нахождения или места жительства лицензиата	141011, Московская обл., г. Мытищи, Фуражный проезд, влад. 4, стр. 2, пом. 2
Адрес(а) мест(а) осуществления лицензируемого вида деятельности	141011, Московская обл., г. Мытищи, Фуражный проезд, влад. 4, стр. 2, пом. 2
Виды работ, услуг по лицензируемому виду деятельности	б; д; е4; е5; е6
Номер и дата приказа о предоставлении, переоформлении, прекращении лицензии	55-л от 28.02.2020

[1] https://reestr.fstec.ru/index.php/regview1?guid=9dcf5083-19e7-434a-a7eb-da844079f42d

Реализация мер Приказа ФСТЭК № 21 в ИСПДн «Консоль.Про»

Идентификатор	Требование	Описание требуемого состояния	Статус[2]
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	**Технически:** Требование реализуется встроенными механизмами операционных систем (далее – ОС), прикладного программного обеспечения (далее – ПО) и платформы Kubernetes **Организационно:** Правила и процедуры управления учетными записями пользователей регламентированы в внутренних нормативных документах (далее – ВНД) Компании	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО и платформы Kubernetes **Организационно:** Правила и процедуры управления идентификаторами регламентированы в ВНД Компании	+
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	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО и платформы Kubernetes **Организационно:** Правила и процедуры управления средствами аутентификации регламентированы в ВНД Компании	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО и платформы Kubernetes	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО и платформы Kubernetes	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО и платформы Kubernetes **Организационно:** Правила и процедуры управления учетными записями пользователей регламентированы в ВНД Компании	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись,	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО и платформы Kubernetes **Организационно:** Правила и процедуры управления учетными записями	+

[2] «+» – требование выполнено; «+ -» – требование выполнено не полностью; «–» – требование не выполнено.

Идентификатор	Требование	Описание требуемого состояния	Статус[2]
	выполнение или иной тип) и правил разграничения доступа	пользователей регламентированы в ВНД Компании. Разграничение доступа реализуются с учетом матриц доступа	
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	**Технически:** Реализуется с помощью технологии yandex virtual private cloud с заданными правилами маршрутизации и организацией всего исходящего трафика через прокси-сервер. Также используется межсетевой экран	**+**
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО и платформы Kubernetes **Организационно:** Правила и процедуры управления учетными записями пользователей регламентированы в ВНД Компании	**+**
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО и платформы Kubernetes **Организационно:** Разграничение доступа реализуются с учетом матриц доступа	**+**
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО и систем управления базами данных (далее – СУБД)	**+**
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО и платформы Kubernetes	**+**
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО и платформы Kubernetes	**+**
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	**Технически:** Требование реализуется при удаленном подключении по зашифрованным каналам связи с помощью VPN технологий	**+**
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного	Не применимо	

Идентификатор	Требование	Описание требуемого состояния	Статус[2]
	доступа		
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	**Организационно:** Правила использования в информационной системе мобильных технических средств регламентированы в ВНД Компании	**+**
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	**Организационно:** Правила и процедуры управления взаимодействием с внешними ИС регламентированы в ВНД Компании	**+**
IV. Защита машинных носителей персональных данных (ЗНИ)			
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	**Технически:** Требования реализуется с помощью специализированного ПО позволяющего исключить возможность восстановления ПДн при их уничтожении с машинных носителей **Организационно:** Процедуры уничтожения (стирания) или обезличивания персональных данных на машинных носителях, а также контроля уничтожения (стирания) или обезличивания регламентированы в ВНД Компании	**+**
V. Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	**Технически:** Реализуется регистрация событий, связанных с действиями работников и администраторов при работе с прикладным ПО на уровне журналов аудита, а также в журналах аудита СУБД, ОС и среды виртуализации **Организационно:** Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется исходя из возможностей реализации угроз безопасности ПДн	**+**
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	**Технически:** Реализуется регистрация событий, связанных с действиями работников и администраторов при работе с прикладным ПО на уровне журналов аудита, а также в журналах аудита СУБД, ОС и среды виртуализации **Организационно:** Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется исходя из возможностей реализации угроз безопасности ПДн	**+**
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	**Технически:** Реализуется регистрация событий, связанных с действиями работников и администраторов при работе с прикладным ПО на уровне журналов аудита, а также в журналах аудита СУБД, ОС и среды виртуализации	**+**

Идентификатор	Требование	Описание требуемого состояния	Статус[2]
		Организационно: Правила и процедуры сбора, записи и хранения информации о событиях безопасности регламентированы в ВНД Компании	
РСБ.7	Защита информации о событиях безопасности	**Организационно:** Правила и процедуры защиты информации о событиях безопасности регламентированы в ВНД Компании	**+**
VI. Антивирусная защита (АВЗ)			
АВЗ.1	Реализация антивирусной защиты	**Технически:** Требование реализовано с помощью применения средств антивирусной защиты **Организационно:** Правила и процедуры антивирусной защиты ИСПДн регламентированы в ВНД Компании	**+**
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	**Технически:** Требование реализовано с помощью применения встроенного функционала используемых средств антивирусной защиты **Организационно:** Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) регламентированы в ВНД Компании	**+**
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)			
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	**Технически:** В Компании применяются open source утилиты для периодического контроля отсутствия и оперативного устранения известных уязвимостей. Сканирование осуществляется на периодической основе Директором по ИБ, в случае выявления уязвимостей они устраняются и осуществляется повторное сканирование. Также реализовано взаимодействие с «Bug Bounty» платформой, на момент выполнения оценки соответствия, с помощью данной платформы уязвимости не выявлены **Организационно:** Правила и процедуры выявления, анализа и устранения уязвимостей регламентированы в ВНД Компании	**+**
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	**Технически:** Требование реализуется встроенными механизмами ОС, прикладного ПО, платформы Kubernetes и используемых средств защиты информации **Организационно:** Правила и процедуры установки и обновления ПО регламентированы в ВНД Компании	**+**
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и	**Технически:** Требование реализуется с помощью встроенных механизмов используемого ПО и средств защиты информации **Организационно:** В Компании утвержден План мероприятий по обеспечению	**+**

Идентификатор	Требование	Описание требуемого состояния	Статус[2]
	средств защиты информации	безопасности ПДн	
АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	**Организационно:** В компании утвержден План мероприятий по обеспечению безопасности ПДн	**+**
XI. Защита среды виртуализации (ЗСВ)			
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Не применимо к Компании т.к. защитные механизмы реализуются платформой «Яндекс.Облако»	
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	**Технически:** Требование реализуется с помощью платформы Kubernetes	**+**
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	**Технически:** Требование реализуется с помощью платформы Kubernetes	**+**
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	**Технически:** Требование реализовано с помощью применения средств антивирусной защиты	**+**
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	**Технически:** Сегментация сети реализована с помощью технологии Yandex Virtual Private Cloud. Выделены следующие сегменты: • производственный (yandex-cloud/production); • разработка и тестирование (yandex-cloud/staging); • безопасность (yandex-cloud/security).	**+**
XII. Защита технических средств (ЗТС)			
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	Неприменимо к Компании т.к. указанный контроль реализован на уровне обеспечения физической безопасности ЦОД	

Идентификатор	Требование	Описание требуемого состояния	Статус[2]
	помещения и сооружения, в которых они установлены		
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	**Организационно:** В ВНД Компании регламентировано размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	**+**
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
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	**Технически:** Требование реализуется путем использования зашифрованных каналов связи в случаях передачи ПДн за пределы контролируемой зоны (htpps, tls, OpenVPN)	**+**
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Неприменимо к Компании т.к. отсутствуют технологии беспроводных соединений	
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)			
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	**Организационно:** В ВНД Компании регламентирована процедура управления изменениями в информационных системах	**+**
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	**Организационно:** В ВНД Компании регламентирована процедура управления изменениями в информационных системах	**+**
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	**Организационно:** В ВНД Компании регламентирована процедура управления изменениями в информационных системах	**+**

Идентификатор	Требование	Описание требуемого состояния	Статус[2]
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	**Организационно:** В ВНД Компании регламентирована процедура управления изменениями в информационных системах	**+**