УТВЕРЖДЕНА
приказом АНО ДПО «Корпоративный университет РЖД»
от «07» июня 2023 г. №КУ-47

ЧАСТНАЯ МОДЕЛЬ УГРОЗ
безопасности персональных данных в информационной системе персональных данных АНО ДПО «Корпоративный университет РЖД»

г. Москва, г. Щербинка
2023 г.

1. Общие положения

Настоящая Частная модель угроз безопасности персональных данных (далее – Модель угроз), в информационной системе персональных данных Корпоративного университета РЖД (далее - ИСПДн), разработана на основании следующих документов:

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

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 14 февраля 2008 г.);

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.)

Частная модель угроз используется при разработке системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн.

2. Основные понятия

В настоящем документе используются следующие понятия и термины:

1.	Корпоративный университет РЖД	Автономная некоммерческая организация дополнительного профессионального образования «Корпоративный университет РЖД»
2.	ПДн	Персональные данные
3.	ИСПДн	Информационная система персональных данных
4.	НСД	Несанкционированный доступ
5.	ЦИБ	Департамент управления информационной безопасностью ОАО «РЖД»

3. Общее описание информационно-технологической структуры

3.1. Описание информационно-технологической структуры

Распределенность инфраструктуры.

Университет имеет подключение к локальной вычислительной сети ОАО «РЖД» – сети передачи данных (СПД), на основании основного договора между ОАО «РЖД» и АНО ДПО «Корпоративный университет РЖД», в соответствии с соглашением об электронном обмене данными №69 от 06 мая 2015 г., а также дополнительным соглашением к нему №1

от 30 августа 2016 г. В СПД университет имеет подключение к следующим информационным системам:

ЕК АСУТР – Единая корпоративная информационная система управления трудовыми ресурсами;

ЕАСД – Единая автоматизированная система документооборота;

ЭПС – Электронная почтовая система ОАО «РЖД».

Также университет имеет собственную локальную вычислительную сеть, имеющую подключение к сети Internet. К сети подключены офисы университета, расположенные по адресам:

г. Москва, г. Щербинка, Бутовский тупик, 1а;

ул. Мясницкая, 48;

ул. Нижегородская, 3аС1.

Назначение используемых в организации серверов.

Сервер 1С – необходим для работы модулей 1С Бухгалтерия, 1С Зарплата и кадры, 1С Университет.

Сервер Web Tutor – необходим для дистанционного обучения слушателей.

Серверы для резервного копирования.

Серверы антивирусной защиты.

Файловые серверы.

Серверы доменной среды.

Логическое и(или) физическое разделение сегментов сети.

Работа в системе 1С организована с помощью терминального сервера, который служит для удалённого обслуживания пользователей с предоставлением рабочего стола.

Система Web Tutor включает рабочие места администратора и пользователя.

Наличие подключение к сетям общего доступа.

Система 1С и система Web Tutor имеют подключение к сети общего доступа.

3.2. Меры физической защиты

Контроль доступа в офисы университета осуществляется следующим образом:

г. Москва, г. Щербинка, Бутовский тупик, 1а и ул. Нижегородская, 3аС1 – контроль охраны наличия входящего в списке работников, которым доступен вход;

ул. Мясницкая, 48 – доступ по пропускам.

В офисах установлены камеры наблюдения – обязательно на входах, а также в некоторых аудиториях.

3.3. Технические средства и методы защиты информации

Используемые типы средств защиты, их наименования, модели и версии.

Антивирусное программное обеспечение Kaspersky и защита сети с помощью межсетевого экрана файрвол.

Компоненты, на которых установлены средства защиты.

Серверы, рабочие места.

Сведения о парольной политике.

Доступ в системы осуществляется по индивидуальному логину и паролю.

Сведения об осведомленности пользователей по вопросам информационной безопасности.

Каждому работнику осуществляется рассылка информационных материалов и нормативных документов в области информационной безопасности, направленных на университет в ЕАСД.

4. Описание информационных систем

В корпоративном университете РЖД выделяются следующие ИСПДн:

1С Университет;

Система дистанционного обучения WebTutor (СДО WebTutor);

1С Зарплата и кадры.

Описание ИСПДн университета приведены в таблицах 1, 2 и 3.

Таблица 1

Описание ИСПДн 1С Университет

1.	Назначение и функционал системы	Хранение и обработка персональных данных слушателей, автоматизация процесса организации обучения
2.	Состав обрабатываемых ПДн	Определен в «ОП_30 Порядок обработки и обеспечения режима защиты персональных данных слушателей», утв. Приказом №КУ-40 от 09.09.2017г.
3.	Состав компонентов системы	Терминальный сервер для удалённого обслуживания пользователя с предоставлением рабочего стола
4.	Наличие подключения к сетям общего доступа	Присутствует
5.	Системы, с которыми осуществляется взаимодействие	Отсутствует
6.	Территориальное расположение системы	Офис по адресу ул. Мясницкая, 48
7.	Сведения о включении в доменную структуру	Доменная структура с сертификатом проверки пользователей и авторизацией логин-пароль
8.	Способы получения доступа к системе, метода идентификации и аутентификации	Индивидуальный логин и пароль создается работником Центра информационных технологий на основе запроса руководителя подразделения университета
9.	Используемые средства и методы защиты	Антивирусное программное обеспечение Kaspersky и защита сети с помощью межсетевого экрана файрвол

Таблица 2

Описание ИСПДн Web Tutor

1.	Назначение и функционал системы	Реализация дистанционного обучения слушателей
2.	Состав обрабатываемых ПДн	ФИО, должность, дата рождения, адрес электронной почты

3.	Состав компонентов системы	Рабочее место администратора базы данных, который осуществляется загрузку персональных данных слушателей и генерирует логин-пароль. Рабочее место слушателя, который осуществляет работу в личном кабинете. Рабочее место методиста университета, который осуществляет проверку работы слушателя в личном кабинете
4.	Наличие подключения к сетям общего доступа	Присутствует
5.	Системы, с которыми осуществляется взаимодействие	Отсутствуют
6.	Территориальное расположение системы	Офис по адресу г. Москва, г. Щербинка, Бутовский тупик, 1а
7.	Сведения о включении в доменную структуру	Привязка к домену сайта curzd.ru
8.	Способы получения доступа к системе, метода идентификации и аутентификации	Индивидуальный логин и пароль для администратора - работника университета - создается работником Центра информационных технологий на основе запроса руководителя подразделения университета. Индивидуальный логин и пароль для слушателя генерируется автоматически при загрузке информации о пользователях в систему
9.	Используемые средства и методы защиты	Антивирусное программное обеспечение Kaspersky и защита сети с помощью межсетевого экрана файрвол

Таблица 3

Описание ИСПДн 1С Зарплата и кадры

1.	Назначение и функционал системы	Ведение кадрового учета

2.	Состав обрабатываемых ПДн	Определен в «ОП_29 Порядок обработки и обеспечения режима защиты персональных данных работников АНО ДПО «Корпоративный университет «РЖД», утв. Приказом №КУ-40 от 09.09.2017г.
3.	Состав компонентов системы	Терминальный сервер для удалённого обслуживания пользователя с предоставлением рабочего стола
4.	Наличие подключения к сетям общего доступа	Присутствует
5.	Системы, с которыми осуществляется взаимодействие	Отсутствуют
6.	Территориальное расположение системы	Офис по адресу ул. Мясницкая, 48
7.	Сведения о включении в доменную структуру	Доменная структура с сертификатом проверки пользователей и авторизацией логин-пароль
8.	Способы получения доступа к системе, метода идентификации и аутентификации	Индивидуальный логин и пароль создается работником Центра информационных технологий на основе запроса руководителя подразделения университета
9.	Используемые средства и методы защиты	Антивирусное программное обеспечение Kaspersky и защита сети с помощью межсетевого экрана файрвол

5. Определение актуальных угроз безопасности персональных данных в ИСПДн Корпоративного университета РЖД

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Актуальность угрозы определяется следующими параметрами:

– уровень исходной защищенности ИСПДн;

– частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных

характеристик ИСПДн. Характеристики ИСПДн 1С Университет, ИСПДн Web Tutor, 1С Зарплата и кадры одинаковы и приведены в таблице 4.

Таблица 4

Показатели исходной защищенности ИСПДн

№	Параметр	Значение	Уровень защищенности
1	Территориальное размещение	Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации	средний
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	средний
3	Встроенные (легальные) операции с записями баз персональных данных	запись, удаление, сортировка	средний
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	высокий
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая	низкий

		идентифицировать субъекта ПДн)	
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, не предоставляющие никакой информации	высокий

Значению уровня защищенности «Высокий» соответствуют 2 характеристики, значению уровня «Средний» - 4 характеристики, значению уровня «Низкий» - 1 характеристика. Таким образом, числовой коэффициент исходной защищенности ИСПДн **Y1 соответствует значению 5 - средняя степень исходной защищенности.**

В таблице ниже приведены данные об оценке актуальности угроз. Для каждой угрозы определяется вероятность реализации угрозы Y2 и соответствующий коэффициент:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом этого реализуемость каждой угрозы Y рассчитывается по формуле:

$Y = (Y1 + Y2) / 20$.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если $0 \leq Y \leq 0,3$, то возможность реализации угрозы признается низкой;

если $0,3 < Y \leq 0,6$, то возможность реализации угрозы признается средней;

если $0,6 < Y \leq 0,8$, то возможность реализации угрозы признается высокой;

если $Y < 0,8$, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов определяется вербальный показатель опасности для рассматриваемой ИСПДн.

Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 5.

Таблица 5

Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Состав угроз определен следующим образом. На основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» установлена типовая модель угроз безопасности, актуальная для университета: Типовая модель угроз безопасности персональных данных, обрабатываемых в распределенных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и(или) сетям международного информационного обмена.

Для данной типовой модели возможна реализация следующих УБПДн:

Таблица 6

Таблица угроз и их характеристики

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность
Угрозы утечки информации по техническим каналам				
Угрозы утечки акустической (речевой) информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы утечки видовой информации	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы утечки информации по каналу ПЭМИН	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы НСД к ПДн непосредственно в ИСПДн				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	маловероятно (0)	низкая (0.25)	средняя	неактуальная
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	маловероятно (0)	низкая (0.25)	средняя	неактуальная
Угрозы внедрения вредоносных программ	средняя вероятность (5)	средняя (0.5)	низкая	неактуальная
Сетевые угрозы				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации	низкая вероятность (2)	средняя (0.35)	средняя	актуальная

Угрозы выявления паролей	низкая вероятность (2)	средняя (0.35)	средняя	актуальная
Угрозы удаленного запуска приложений	низкая вероятность (2)	средняя (0.35)	средняя	актуальная
Угрозы внедрения по сети вредоносных программ	низкая вероятность (2)	средняя (0.35)	низкая	неактуальная
Угрозы из внешних сетей				
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	низкая вероятность (2)	средняя (0.35)	средняя	актуальная
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы выявления паролей	низкая вероятность (2)	средняя (0.35)	средняя	актуальная
Угрозы получения НСД путем подмены доверенного объекта	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы типа "Отказ в обслуживании"	низкая вероятность (2)	средняя (0.35)	средняя	актуальная
Угрозы удаленного запуска приложений	маловероятно (0)	низкая (0.25)	низкая	неактуальная
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	средняя (0.5)	средняя	актуальная

6. Анализ внутренних бизнес-процессов Корпоративного университета на предмет наличия угроз безопасности ПДн при обработке вне ИСПДн

Все процессы, связанные с обработкой ПДн в университете, делятся на 3 группы:

1. Обмен информацией, содержащей ПДн, с внешними организациями: получение от заказчика списков слушателей, предоставление заказчику данных об успеваемости слушателей и результатах обучения.
2. Обмен информацией, содержащей ПДн, между подразделениями университета: передача списков слушателей для загрузки в систему дистанционного обучения (ИСПДн WebTutor), передача списков слушателей для организации обучения и т.д.
3. Обработка ПДн на локальных рабочих местах.

Для процессов первой группы используются следующие информационные системы:

1. Корпоративная электронная почта ОАО «РЖД».
2. ЕАСД.
3. ЕК АСУТР.
4. Внешняя электронная почта.

Из перечисленных информационных систем только ЕАСД входит в перечень систем, допустимых для передачи персональных данных в электронном виде, определенном в информационном письме Департамента управления информационной безопасностью ОАО «РЖД», а также допустимым является получение ПДн из ЕК АСУТР.

Для процессов второй группы используются следующие информационные системы:

1. Корпоративная электронная почта ОАО «РЖД».
2. Внешняя электронная почта.

Перечисленные информационные системы не входят в перечень систем, допустимых для передачи персональных данных в электронном виде, определенном в информационном письме Департамента управления информационной безопасностью ОАО «РЖД».

Для третьей группы процессов актуальной является угроза отсутствия блокировки учетной записи при покидании рабочего места работником.

7. Мероприятия по предотвращению угроз безопасности ПДн

№	Актуальные угрозы	Мероприятия по предотвращению угроз
1.	Сетевые угрозы: Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации; Угрозы выявления паролей; Угрозы удаленного запуска приложений; Угрозы из внешних сетей: Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации; Угрозы выявления паролей; Угрозы типа "Отказ в обслуживании"; Угрозы внедрения по сети вредоносных программ	Реализация системы с установленными для передачи информации ограниченного доступа сертифицированными механизмами защиты, например, ViPNet и других, отвечающих требованиям безопасности информации, рекомендованными ЦИБ ОАО «РЖД».
2.	Угрозы безопасности ПДн при обмене ПДн с внешними организациями и подразделениями университета через информационные системы, не включенные в перечень систем, допустимых для передачи персональных данных в электронном виде, определенном в информационном письме Департамента управления	Организация доступа работникам университета к системам, рекомендованным для передачи в электронном виде информации, содержащие персональные данные, в письме Департамента управления информационной безопасностью ОАО «РЖД». Временные мероприятия: 1. Передача документов, содержащих ПДн, через ЕАСД с обязательной пометкой «Ограниченный доступ».

	информационной безопасностью ОАО «РЖД»	2. Передача ПДн на съемных машинных носителях информации с соблюдением требований нормативных документов ОАО «РЖД» по информационной безопасности и делопроизводству. 3. Получение информации из ЕК АСУТР.
3.	Угроза отсутствия блокировки учетной записи при покидании рабочего места работником	1. Установить периодичность смены пароля учетной записи. 2. Провести обучение работников о необходимости блокировки учетной записи при покидании рабочего места более чем на 5 минут или при отсутствии зрительного контроля доступа постороннего лица к учетной записи. 3. Провести обучение руководителей о необходимости контроля блокировки учетной записи работниками при покидании рабочего места

Идентификатор документа 816c272b-0075-4815-9e89-d1c0bd9a1915

Документ подписан и передан через оператора ЭДО АО «ПФ «СКБ Контур»

	Организация, сотрудник	Доверенность: рег. номер, период действия и статус	Сертификат: серийный номер, период действия	Дата и время подписания
Подписи отправителя:	АНО ДПО "КОРПОРАТИВНЫЙ УНИВЕРСИТЕТ РЖД" Баскин Роман Валерьевич, ДИРЕКТОР	Не требуется для подписания	0135B49500C8AF9FBB4073E5B242B53DE9 с 17.03.2023 11:55 по 17.06.2024 11:55 GMT+03:00	07.05.2024 17:28 GMT+03:00 Подпись соответствует файлу документа
Подписи получателя:	АНО ДПО "КОРПОРАТИВНЫЙ УНИВЕРСИТЕТ РЖД" Баскин Роман Валерьевич, ДИРЕКТОР	Не требуется для подписания	0135B49500C8AF9FBB4073E5B242B53DE9 с 17.03.2023 11:55 по 17.06.2024 11:55 GMT+03:00	07.05.2024 17:28 GMT+03:00 Подпись соответствует файлу документа