УТВЕРЖДАЮ
Председатель Правления
КПК «_____»
ФИО

_____
« » _____ 20 __ г.

ЧАСТНАЯ МОДЕЛЬ УГРОЗ ИСПДН "_____: СОТРУДНИКИ И КОНТРАГЕНТЫ"

Настоящий документ подготовлен в рамках выполнения работ по проектированию системы защиты персональных данных для информационной системы персональных данных №1 «_____: сотрудники и контрагенты» (далее – ИСПДн КК:СК).

ИСПДн КК:СК предназначена для решения задач управления персоналом и реализации уставных целей. Объекты КПК «_____» размещаются на территории г. _____. В составе ИСПДн КК:СК функционирует 20 АРМ и 2 сервера. Рассматриваемая ИСПДн КК:СК имеет подключение к сетям общего пользования и международного обмена. Все компоненты ИСПДн КК:СК находятся на одном объекте, внутри контролируемой зоны. Обработка персональных данных ведется в многопользовательском режиме, без ограничения прав доступа. Все технические средства находятся в пределах РФ. К персональным данным предъявляются требования целостности и доступности.
В ИСПДн КК:СК обрабатываются данные второй категории персональных данных. Объем обработки не превышает 1 000 записей о субъектах ПДн.

При входе в систему и выдаче запросов на доступ проводится аутентификация пользователей ИСПДн КК:СК. Все пользователи имеют собственные роли: администратор безопасности, пользователи с правом чтения-записи, пользователи с правом чтения данных.

Модель вероятного нарушителя безопасности персональных данных
По признаку принадлежности к ИСПДн КК:СК все нарушители делятся на две группы: внутренние, имеющие непосредственный доступ к ИСПДн, и внешние, без прямого доступа к ИСПДн - реализующие угрозы из внешних сетей связи.

Внешними нарушителями могут быть:

- криминальные структуры;
- недобросовестные конкуренты.

Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ (НСД) к каналам связи, выходящим за пределы служебных помещений;

- осуществлять НСД через автоматизированные рабочие места, подключенные к сетям связи общего пользования;
- осуществлять НСД к информации с использованием специальных программных воздействий, включая вредоносные программы и программы-закладки.

Показатели исходной защищенности ИСПДн НК:КК

Справочно: необязательно полностью публиковать все поля данной таблицы, вполне достаточно включить в документ только те строки, в которых будут отмечены рабочие значения, в данном документе рабочие значения маркированы знаками “плюс”, отличающимися размером и цветом.

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению: распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего			

пользования: ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных: чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4. По разграничению доступа к персональным данным:	–	+	–
ИСПДн, к которой имеют доступ определенные переченем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;			
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн:	–	–	+

интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.); ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации; ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	+ – –	– + –	– – +
7. По объему ПДн, которые предоставляются сторонним	–	–	+

пользователям ИСПДн без предварительной обработки: ИСПДн, предоставляющая всю базу данных с ПДн;			
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации.	+	–	–

ИСПДн КК:СК имеет средний уровень исходной защищенности, так как не менее 70% характеристик соответствуют уровню не ниже «средний». Показатель исходной защищенности Y_1=5.

Вероятность реализации угроз безопасности ПДн

Справочно: под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для ИСПДн в складывающихся условиях обстановки. Коэффициент вероятности реализации (Y_2) определяется по 4 вербальным градациям:

- *маловероятно* – отсутствуют объективные предпосылки для осуществления угрозы (Y_2=0);
- *низкая вероятность* – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют её реализацию (Y_2=2);
- *средняя вероятность* - объективные предпосылки для реализации угрозы существуют, но принятые меры безопасности ПДн недостаточны (Y_2=5);
- *высокая вероятность* - объективные предпосылки для реализации угрозы существуют и меры обеспечения безопасности ПДн не приняты (Y_2=10).

Угроза безопасности ПДн	**Коэффициент вероятности реализации (Y2)**
угроза модификации BIOS	2
угроза перехвата управления загрузкой	0
угроза НСД с применением стандартных функций операционной системы	2
угроза НСД с помощью прикладной программы	2

угроза НСД с с применением специально созданных для этого программ	0
угроза НСД при передаче информации по внешним каналам	0
угроза утечки информации при удаленном доступе к информационным ресурсам	0
угроза утечки информации с использованием копирования её на съемные носители	5
угроза утечки информации посредством её печати на множительной технике	2
угроза утечки информации за счет её несанкционированной передачи по каналам связи	2
угроза внедрения вредоносных программ с использованием съемных носителей	2
угроза «Анализ сетевого трафика»	2
угроза сканирования открытых портов, служб и соединений	2
угроза обхода системы идентификации и аутентификации сообщений	0
угроза обхода системы идентификации и сетевых объектов	2
угроза внедрения ложного объекта сети	2
угроза навязывания ложного маршрута	2
угроза перехвата и взлома паролей	2
угроза подбора паролей доступа	2
угроза типа «Отказ в обслуживании»	2
угроза внедрения троянских программы	2
угроза атаки типа «Переполнение буфера»	2
угроза удаленного запуска приложений с использованием средств удаленного администрирования	2
угроза внедрения вредоносных программ через почтовые сообщения	2
угроза внедрения вредоносных программ через обмен и загрузку файлов	2

угроза заражения сетевыми червями, использующими уязвимости сетевого ПО	2

Оценка возможности реализации и опасности угроз

По итогам оценки уровня исходной защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы.

Справочно: Формула расчета коэффициента реализуемости угрозы: $Y=(Y_1+Y_2)/20$.

Возможность реализации угрозы определяется по следующим диапазонам:

0>Y>0,3 - низкая

0,3>Y>0,6 - средняя

0,6>Y>0,8 - высокая

Y>0,8 – высокая

Одновременно производится оценка опасности, которая определяется на основе опроса специалистов по вербальным показателям опасности с тремя значениями:

- *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.

Угроза безопасности ПДн	**Коэффициент реализуемости угрозы (Y)**	**Возможность реализации угрозы**	**Оценка опасности угрозы**
угроза модификации BIOS	0,35	средняя	низкая
угроза перехвата управления загрузкой	0,25	низкая	низкая
угроза НСД с применением стандартных функций операционной системы	0,35	средняя	средняя
угроза НСД с помощью прикладной программы	0,35	средняя	низкая
угроза НСД с с применением специально созданных для этого программ	0,25	низкая	низкая
угроза НСД при передаче информации по внешним каналам	0,25	низкая	высокая

угроза утечки информации при удаленном доступе к информационным ресурсам	0,25	низкая	высокая
угроза утечки информации с использованием копирования её на съемные носители	0,5	средняя	высокая
угроза утечки информации посредством её печати на множительной технике	0,35	средняя	высокая
угроза утечки информации за счет её несанкционированной передачи по каналам связи	0,35	средняя	низкая
угроза внедрения вредоносных программ с использованием съемных носителей	0,35	средняя	средняя
угроза «Анализ сетевого трафика»	0,35	средняя	средняя
угроза сканирования открытых портов, служб и соединений	0,35	средняя	низкая
угроза обхода системы идентификации и аутентификации сообщений	0,25	низкая	низкая
угроза обхода системы идентификации и сетевых объектов	0,35	средняя	низкая
угроза внедрения ложного объекта сети	0,35	средняя	низкая
угроза навязывания ложного маршрута	0,35	средняя	низкая
угроза перехвата и взлома паролей	0,35	средняя	низкая
угроза подбора паролей доступа	0,35	средняя	средняя
угроза типа «Отказ в обслуживании»	0,35	средняя	низкая
угроза внедрения троянских	0,35	средняя	средняя

программ			
угроза атаки типа «Переполнение буфера»	0,35	средняя	низкая
угроза удаленного запуска приложений с использованием средств удаленного администрирования	0,35	средняя	низкая
угроза внедрения вредоносных программ через почтовые сообщения	0,35	средняя	средняя
угроза внедрения вредоносных программ через обмен и загрузку файлов	0,35	средняя	низкая
угроза заражения сетевыми червями, использующими уязвимости сетевого ПО	0,35	средняя	низкая

Перечень актуальных угроз ИСПДн КК:СК
Отнесение угрозы к актуальной производится по правилам, приведенным в Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России 14.02.2008, по таблице:

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

В соответствии с правилами отнесения угроз безопасности к актуальным для ИСПДн КК:СК существуют следующие характеристики актуальности угроз:

Угроза безопасности ПДн	Актуальность угрозы
угроза модификации BIOS	неактуальная
угроза перехвата управления загрузкой	неактуальная
угроза НСД с применением стандартных функций операционной системы	неактуальная
угроза НСД с помощью прикладной программы	неактуальная
угроза НСД с с применением специально созданных для этого программ	неактуальная
угроза НСД при передаче информации по внешним каналам	актуальная
угроза утечки информации при удаленном доступе к информационным ресурсам	актуальная
угроза утечки информации с использованием копирования её на съемные носители	актуальная
угроза утечки информации посредством её печати на множительной технике	актуальная
угроза утечки информации за счет её несанкционированной передачи по каналам связи	неактуальная
угроза внедрения вредоносных программ с использованием съемных носителей	актуальная
угроза «Анализ сетевого трафика»	актуальная
угроза сканирования открытых портов, служб и соединений	неактуальная
угроза обхода системы идентификации и аутентификации сообщений	неактуальная
угроза обхода системы идентификации и сетевых объектов	неактуальная
угроза внедрения ложного объекта сети	неактуальная
угроза навязывания ложного маршрута	неактуальная
угроза перехвата и взлома паролей	неактуальная
угроза подбора паролей доступа	неактуальная
угроза типа «Отказ в обслуживании»	неактуальная

угроза внедрения троянских программ	актуальная
угроза атаки типа «Переполнение буфера»	неактуальная
угроза удаленного запуска приложений с использованием средств удаленного администрирования	неактуальная
угроза внедрения вредоносных программ через почтовые сообщения	актуальная
угроза внедрения вредоносных программ через обмен и загрузку файлов	неактуальная
угроза заражения сетевыми червями, использующими уязвимости сетевого ПО	неактуальная

Таким образом, актуальными угрозами безопасности ПДн в ИСПДн КК:СК являются:

- угроза НСД с применением стандартных функций операционной системы;
- угроза НСД при передаче информации по внешним каналам;
- угроза утечки информации при удаленном доступе к информационным ресурсам;
- угроза утечки информации с использованием копирования её на съемные носители;
- угроза утечки информации посредством её печати на множительной технике;
- угроза внедрения вредоносных программ с использованием съемных носителей;
- угроза «Анализ сетевого трафика»;
- угроза внедрения троянских программ;
- угроза внедрения вредоносных программ через почтовые сообщения.

Созданная и функционирующая в настоящий момент система информационной безопасности ООО «Наша компания», помимо комплекса организационных мер использует следующие средства защиты информации:

- средства антивирусной защиты Kaspersky Total Space Security;
- программный комплекс «Межсетевой экран Ideco ICS»;
- средства управления доступом в систему (Active Directory);
- методы и средства аутентификации пользователей на основе usb-ключей;
- средства криптографической защиты информации.

Использование в составе системы информационной безопасности данных средств позволяет с уверенностью говорить о том, что их заявленный функционал сможет достаточно эффективно обеспечить защиту ПДн и существенно снизить вероятность реализации следующих актуальных угроз:

- угроза НСД при передаче информации по внешним каналам;
- угроза утечки информации при удаленном доступе к информационным ресурсам;
- угроза внедрения вредоносных программ с использованием съемных носителей;
- угроза «Анализ сетевого трафика»;
- угроза внедрения троянских программ.

Заключение

Результаты моделирования угроз безопасности ПДн показывают, что в ИСПДн КК:СК требуется проведение дополнительных мероприятий по доработке существующей системы информационной безопасности для организации противодействия следующим актуальным угрозам безопасности ПДн:

- угроза НСД с применением стандартных функций операционной системы;
- угроза утечки информации с использованием копирования её на съемные носители;
- угроза утечки информации посредством её печати на множительной технике.

Построенная модель безопасности применима к существующему состоянию ИСПДн КК:СК при условии соблюдения основных (базовых) исходных данных:

- технические средства находятся в пределах контролируемой зоны;
- ИСПДн отделена от сетей общего пользования средствами внутрисетевого экранирования;
- отсутствует возможность неконтролируемого пребывания посторонних лиц в служебных помещениях ИСПДн.

В случае несоблюдения и/или изменения вышеуказанных условий Модель угроз безопасности ПДн в ИСПДн КК:СК должна быть пересмотрена.