Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение
«Политехнический колледж городского хозяйства»

Организационно-правовая документация

УТВЕРЖДЕНА
приказом директора
от 10.10. 2023
№ 776 - ОД

ЧАСТНАЯ МОДЕЛЬ УГРОЗ

БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ «ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ ГОРОДСКОГО ХОЗЯЙСТВА»

Санкт-Петербург - 2023

	Должность	Фамилия И.О.	Подпись	Дата
Разработал	Специалист по защите информаций	Бабин С.А.		06.10.23
Согласовано	Зам. директора по ПО	Бурдин Е.В.		06.10.23
Согласовано	Начальник отдела ИО и ПП	Ваганов С.В.		05.10.23
Согласовано	Начальник отдела ДОУ	Шорина А.В.		06.10.23

УТВЕРЖДЕНА
приказом директора
от 10.10 2023
№ 476 -ОД

ЧАСТНАЯ МОДЕЛЬ УГРОЗ
безопасности персональных данных в информационных системах персональных данных Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Политехнический колледж городского хозяйства»

1. Описание систем и сетей и их характеристика как объектов защиты

Сокращения
АРМ – автоматизированное рабочее место;
АС – автоматизированная система;
ВТСС – вспомогательные технические средства и системы;
ИСПДн – информационная система персональных данных;
НСД – несанкционированный доступ;
ОС – операционная система;
ПДн – персональные данные;
ПО – программное обеспечение;
ПЭМИН – побочные электромагнитные излучения и наводки;
СВТ – средства вычислительной техники;
СЗИ – средства защиты информации;
СУБД – система управления базами данных;
УБПДн – угрозы безопасности персональным данным.

1.1 Наименование систем и сетей, для которых разработана модель угроз безопасности информации

1.1.1 Полное наименование информационной системы: Информационная система персональных данных Заказчика, предназначенная для обмена информацией с Федеральной информационной системой обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и Федеральной информационной системой «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении».

Сокращенное наименование информационной системы: ИСПДн «АРМ передачи сведений в ФИС ГИА и Приема и ФИС ФРДО».

Параметры ИСПДн «АРМ передачи сведений в ФИС ГИА и Приема и ФИС ФРДО», влияющие на класс защищенности информационной системы и уровень защищенности ПДн

Категория обрабатываемых персональных данных	иные категории персональных данных субъектов персональных данных, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100000
Тип угроз безопасности персональных данных, актуальных для информационной системы	Угрозы 3-го типа

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» рассматриваемая ИСПДн «АРМ передачи сведений в ФИС ГИА и Приема и ФИС ФРДО» относится к информационным системам, обрабатывающим иные категории персональных данных менее 100000 субъектов ПДн, не являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн «АРМ передачи сведений в ФИС ГИА и Приема и ФИС ФРДО», актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для ИСПДн «АРМ передачи сведений в ФИС ГИА и Приема и ФИС ФРДО» актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн «АРМ передачи сведений в ФИС ГИА и Приема и ФИС ФРДО», на основе анализа угроз безопасности информации, и в соответствии с п.п. 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» в ИСПДн «АРМ передачи сведений в ФИС ГИА и Приема и ФИС ФРДО» необходимо обеспечить четвертый уровень защищенности ПДн.

1.1.2. Полное наименование информационной системы: Государственная информационная система Санкт-Петербурга «Единая информационно-аналитическая система бюджетного (бухгалтерского) учета»

Сокращенное наименование информационной системы: «ГИС ЕИАСБУ».

Параметры ИСПДн «ГИС ЕИАСБУ», влияющие на класс защищенности информационной системы и уровень защищенности ПДн:

Категория обрабатываемых персональных данных	иные категории персональных данных субъектов персональных данных, являющихся сотрудниками оператора, в незначительном количестве специальные категории персональных данных субъектов персональных данных, являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100000
Тип угроз безопасности персональных данных, актуальных для информационной системы	Угрозы 3-го типа

На основании результатов анализа исходных данных, и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» рассматриваемая ИСПДн «ГИС ЕИАСБУ» относится к информационным системам, обрабатывающим

специальные категории персональных данных менее 100000 субъектов ПДн, являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн «ГИС ЕИАСБУ», актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для ИСПДн «ГИС ЕИАСБУ» актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн «ГИС ЕИАСБУ», на основе анализа угроз безопасности информации, и в соответствии с п.п. 11 «Требований к защите персональных данных при их обработке в информационной системе персональных данных «ГИС ЕИАСБУ» необходимо обеспечить третий уровень защищенности ПДн.

1.1.3 Полное наименование информационной системы: Комплексная система обеспечения мониторинга безопасности», входящей в состав государственной информационной системы Санкт-Петербурга «Аппаратно-программный комплекс «Безопасный город.

Сокращенное наименование информационной системы: АС «КСОМБ».

Параметры ИСПДн АС «КСОМБ», влияющие на класс защищенности информационной системы и уровень защищенности ПДн:

Категория обрабатываемых персональных данных	иные категории персональных данных субъектов персональных данных, являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100000
Тип угроз безопасности персональных данных, актуальных для информационной системы	Угрозы 3-го типа

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» рассматриваемая ИСПДн АС «КСОМБ» относится к информационным системам, обрабатывающим иные категории персональных данных менее 100000 субъектов ПДн, являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн АС «КСОМБ», актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для ИСПДн АС «КСОМБ» актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн АС «КСОМБ», на основе анализа угроз безопасности информации, и в соответствии с п.п. 12 «Требований к защите персональных

данных при их обработке в информационных системах персональных данных» в ИСПДн АС «КСОМБ» необходимо обеспечить четвертый уровень защищенности ПДн.

1.1.4 Полное наименование информационной системы: Единая государственная информационная система социального обеспечения.

Сокращенное наименование информационной системы: «ЕГИССО».

Параметры ИСПДн «ЕГИССО», влияющие на класс защищенности информационной системы и уровень защищенности ПДн:

Категория обрабатываемых персональных данных	иные категории персональных данных субъектов персональных данных, являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100000
Тип угроз безопасности персональных данных, актуальных для информационной системы	Угрозы 3-го типа

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» рассматриваемая ИСПДн «ЕГИССО» относится к информационным системам, обрабатывающим иные категории персональных данных менее 100000 субъектов ПДн, являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн «ЕГИССО», актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для ИСПДн «ЕГИССО» актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн «ЕГИССО», на основе анализа угроз безопасности информации, и в соответствии с п.п. 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» в ИСПДн «ЕГИССО» необходимо обеспечить четвертый уровень защищенности ПДн.

1.1.5 Полное наименование информационной системы: Электронная отчетность и документооборот.

Сокращенное наименование информационной системы: «СБИС».

Параметры ИСПДн «СБИС», влияющие на класс защищенности информационной системы и уровень защищенности ПДн:

Категория обрабатываемых персональных данных	иные категории персональных данных субъектов персональных данных, являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100000
Тип угроз безопасности персональных	Угрозы 3-го типа

данных, актуальных для информационной системы	

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» рассматриваемая ИСПДн «СБИС» относится к информационным системам, обрабатывающим иные категории персональных данных менее 100000 субъектов ПДн, являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн «СБИС» актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для ИСПДн «СБИС» актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн «СБИС», на основе анализа угроз безопасности информации, и в соответствии с п.п. 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» в ИСПДн «СБИС» необходимо обеспечить четвертый уровень защищенности ПДн

1.1.6 Полное наименование информационной системы: Личный кабинет организации на сайте Госуслуг»

Сокращенное наименование информационной системы: «ЛКО ГУ».

Параметры ИСПДн «ЛКО ГУ», влияющие на класс защищенности информационной системы и уровень защищенности ПДн:

Категория обрабатываемых персональных данных	иные категории персональных данных субъектов персональных данных, являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100000
Тип угроз безопасности персональных данных, актуальных для информационной системы	Угрозы 3-го типа

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» рассматриваемая ИСПДн «ЛКО ГУ» относится к информационным системам, обрабатывающим иные категории персональных данных менее 100000 субъектов ПДн, являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн «ЛКО ГУ» актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для ИСПДн «ЛКО ГУ» актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн «ЛКО ГУ», на основе анализа угроз безопасности информации, и в

соответствии с п.п. 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» в ИСПДн «ЛКО ГУ» необходимо обеспечить четвертый уровень защищенности ПДн

1.1.7 Полное наименование информационной системы: Система контроля и управления доступом» оператором которой является Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Политехнический колледж городского хозяйства».

Сокращенное наименование информационной системы: «СКУД».

Параметры ИСПДн «СКУД», влияющие на класс защищенности информационной системы и уровень защищенности ПДн:

Категория обрабатываемых персональных данных	иные категории персональных данных субъектов персональных данных, являющихся сотрудниками оператора, и не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100000
Тип угроз безопасности персональных данных, актуальных для информационной системы	Угрозы 3-го типа

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» рассматриваемая ИСПДн «СКУД» относится к информационным системам, обрабатывающим иные категории персональных данных менее 100000 субъектов ПДн, являются сотрудниками оператора, и не являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн «СКУД» актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для ИСПДн «СКУД» актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн «СКУД», на основе анализа угроз безопасности информации, и в соответствии с п.п. 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» в ИСПДн «СКУД» необходимо обеспечить четвертый уровень защищенности ПДн.

1.1.8 Полное наименование информационной системы: официальный сайт образовательной организации в информационно-телекоммуникационной сети «Интернет» - информационный сайт колледжа.

Сокращенное наименование информационной системы: «Сайт колледжа».

Параметры ИСПДн «Сайт колледжа», влияющие на класс защищенности информационной системы и уровень защищенности ПДн:

Категория обрабатываемых	иные категории персональных данных

персональных данных	субъектов персональных данных, являющихся сотрудниками оператора, и не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100000
Тип угроз безопасности персональных данных, актуальных для информационной системы	Угрозы 3-го типа

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» рассматриваемая ИСПДн «Сайт колледжа» относится к информационным системам, обрабатывающим иные категории персональных данных менее 100000 субъектов ПДн, являются сотрудниками оператора, и не являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн «Сайт колледжа» актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для ИСПДн «Сайт колледжа» актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн «Сайт колледжа», на основе анализа угроз безопасности информации, и в соответствии с п.п. 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» в ИСПДн «Сайт колледжа» необходимо обеспечить четвертый уровень защищенности ПДн

1.1.9 Полное наименование информационной системы: автоматизированная бухгалтерская система учета начислений и выплат стипендий студентам – «1С Зарплата и Кадры».

Сокращенное наименование информационной системы: «1С Зарплата и Кадры».

Параметры ИСПДн «1С Зарплата и Кадры», влияющие на класс защищенности информационной системы и уровень защищенности ПДн:

Категория обрабатываемых персональных данных	иные категории персональных данных субъектов персональных данных, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100000
Тип угроз безопасности персональных данных, актуальных для информационной системы	Угрозы 3-го типа

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» рассматриваемая ИСПДн

«1С Зарплата и Кадры» относится к информационным системам, обрабатывающим иные категории персональных данных менее 100000 субъектов ПДн, не являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн «1С Зарплата и Кадры» актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для ИСПДн «1С Зарплата и Кадры» актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн «1С Зарплата и Кадры», на основе анализа угроз безопасности информации, и в соответствии с п.п. 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» в ИСПДн «1С Зарплата и Кадры» необходимо обеспечить четвертый уровень защищенности ПДн.

1.1.10 Полное наименование информационной системы: Комплексная система разработанная на платформе «1С:Предприятие 8.3». для управления средней специальной профессиональной образовательной организацией на всех уровнях управленческой деятельности, в том числе для организации : работы приемной комиссии, учета студентов, составления расписания – «1С Колледж ПРОФ».

Сокращенное наименование информационной системы: «1С Колледж ПРОФ».

Параметры ИСПДн «1С Колледж ПРОФ», влияющие на класс защищенности информационной системы и уровень защищенности ПДн:

Категория обрабатываемых персональных данных	иные категории персональных данных субъектов персональных данных, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100000
Тип угроз безопасности персональных данных, актуальных для информационной системы	Угрозы 3-го типа

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» рассматриваемая ИСПДн «1С Колледж ПРОФ» относится к информационным системам, обрабатывающим иные категории персональных данных менее 100000 субъектов ПДн, не являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн «1С Колледж ПРОФ» актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в

информационной системе, т.е. для ИСПДн «1С Зарплата и Кадры» актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн «1С Колледж ПРОФ», на основе анализа угроз безопасности информации, и в соответствии с п.п. 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» в ИСПДн «1С Колледж ПРОФ» необходимо обеспечить четвертый уровень защищенности ПДн.

1.1.11. Полное наименование информационной системы: программный комплексы, предназначенный для автоматизации основных процессов управления учреждениями системы образования на базе комплекса «Параграф».

Сокращенное наименование информационной системы: «Параграф»

Параметры ИСПДн «Параграф», влияющие на класс защищенности информационной системы и уровень защищенности ПДн:

Категория обрабатываемых персональных данных	иные категории персональных данных субъектов персональных данных, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100000
Тип угроз безопасности персональных данных, актуальных для информационной системы	Угрозы 3-го типа

На основании результатов анализа исходных данных и в соответствии с п. 5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» рассматриваемая ИСПДн «Параграф» относится к информационным системам, обрабатывающим иные категории персональных данных менее 100000 субъектов ПДн, не являются сотрудниками оператора.

Проведенный анализ актуальности угроз позволяет сделать вывод о том, что для ИСПДн «Параграф»» актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе, т.е. для ИСПДн «Параграф» актуальны угрозы 3-го типа.

Таким образом, на основании результатов анализа исходных данных об ИСПДн «Параграф», на основе анализа угроз безопасности информации, и в соответствии с п.п. 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных» в ИСПДн «Параграф» необходимо обеспечить четвертый уровень защищенности ПДн.

1.2 Нормативные правовые акты РФ, в соответствии с которыми функционируют ИСПДн

ИСПДн разрабатывалась в соответствии со следующими нормативно-правовыми актами:

- Конституция Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Бюджетный кодекс Российской Федерации;
- Федеральный закон «О бухгалтерском учете»;
- Федеральный закон «Об образовании»;
- Федеральный закон «Об обязательном пенсионном страховании в Российской Федерации»;
-Федеральный закон «О противодействии коррупции»;
- Федеральный закон «Об архивном деле»;
- Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации»;
- Иные Федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью Оператора.

Правовым основанием обработки персональных данных также являются:
- Устав СПб ГБПОУ «ПКГХ»;
- Действующая редакция Положения о порядке обработки, хранения, использования и защиты персональных данных работников и студентов в Санкт-Петербургском государственном бюджетном образовательном учреждении среднего профессионального образования «Политехнический колледж| городского хозяйства»;
- Договоры, заключаемые между Оператором и субъектами персональных данных;
- Согласие субъектов персональных данных на обработку их персональных данных.

1.3 Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и их правовой режим

ИСПДн указанные в п.1.1 представляет собой информационные системы, объединяющую совокупность средств вычислительной техники, являющихся частью IT-инфраструктуры организации, и предназначенную для обработки персональных данных субъектов ПДн.

Основные цели создания систем:

Указанной в п.1.1.1 настоящего документа:

Система предназначена для ликвидации оборота поддельных документов государственного образца об образовании; обеспечения ведомств и работодателей достоверной информацией о квалификации претендентов на трудоустройство; сокращения числа нарушений и коррупции в

образовательных учреждениях; повышения качества образования за счет обеспечения общественности достоверной информацией о выпускниках. Обеспечивает выполнение следующих функций: сбор, учет, хранение, анализ, систематизация и графическое представление обрабатываемой информации; многокритериальный поиск обрабатываемой информации, фильтрация, отбор информации по заданным пользователем критериям и показателям; предоставление сведений во внешние ИС; логирование входов и выходов пользователя; распределение доступа между пользователями.

Указанной в п.1.1.2: настоящего документа:

Система позволяет подключиться к сервису «1С-Отчетность» для отправки отчетности и обмена другими документами с контролирующими и исполнительными государственными органами: Федеральная налоговая служба РФ, Пенсионный фонд РФ, Фонд социального страхования РФ, Росстат, Росприроднадзор, Федеральное казначейство РФ Федеральная таможенная служба РФ.

Указанной в п.1.1.3: настоящего документа:

Система предназначена для автоматизации деятельности Санкт-Петербургского государственного казенного учреждения «Городской мониторинговый центр» в части сбора, обработки, хранения и предоставления мониторинговой информации о контролируемых объектах.

Указанной в п.1.1.4 настоящего документа:

Является информационной системой, позволяющей получать гражданам и органам власти актуальную информацию о мерах социальной защиты и поддержки, оказываемых из бюджетов всех уровней, как в отношении отдельно взятого человека, так и в целом по стране, а также получать сведения, необходимые органам власти для предоставления мер социальной защиты и поддержки. Система позволяет повысить эффективность государственного управления в области государственной социальной помощи, а также уровень информированности граждан о правах на социальное обеспечение и снизить их физические и временные затраты при получении тех или иных мер социальной поддержки. Обеспечивает возможность применения принципов адресности и критериев нуждаемости при предоставлении мер социальной поддержки. Кроме того, данная система позволит проводить аналитику по интересующим показателям в сфере социальной поддержки граждан и, прогнозировать расходы бюджетов в части выполнения социальных обязательств государства.

Указанной в п.1.1.5 настоящего документа:

В системе собраны решения в ом числе для юридических лиц. Позволяет формировать и направлять отчетность через интернет — система подготовки, проверки и сдачи электронной отчетности через Интернет во все государственные органы. В системе реализованы все возможные бухгалтерские и налоговые отчеты. Система позволяет вести электронный документооборот — обмен документами (договоры, накладные, счета - фактуры, универсальные передаточные документы, акты и прочее) с

контрагентами и внутри компании (задачи, инструкции, приказы, согласования и прочее). В системе реализованы бухгалтерия и учет — позволяет автоматизировать налоговый, бухгалтерский, складской и управленческий учет. ОФД и онлайн-кассы — позволяет передавать чеки в Федеральную налоговую службу РФ через оператора фискальных данных (ОФД). На основе этой информации СБИС строит отчеты, планировать поставки и многое другое. Торги и закупки — сервис помогает организовать работу с торгами: поставщик найдет закупки на электронных торговых площадках и спрогнозирует поведение конкурентов, заказчик (учреждение) — создает запрос предложений, а субподрядчик — сможет стать партнером победителя торгов.

Указанной в п.1.1.6 настоящего документа:

Система позволяет взаимодействовать учреждению с различными государственными органами и позволяет выполнить следующие операции: проверять наличие судебных задолженностей; получение информации о реорганизации юридического лица; сдача отчетных документов в налоговую службу или в другие государственные органы; получение данных о наличии исполнительного производства; оплата штрафов за нарушение правил дорожного движения; получение сертификатов и разрешений, необходимых для ведения бизнеса.

Указанной в п.1.1.7 настоящего документа:

Система реализована на базе аппаратно-программного комплекса: интегрированная система охраны «Орион», предназначенного для организации комплексной охраны различных объектов, и позволяющего: осуществлять запись видео в видеоархив, воспроизведение видеозаписей из архива; осуществлять сбор и отображение статистики адресных датчиков в специализированном программном модуле, а также отображение показаний на планах помещения; осуществлять разграничение прав доступа в соответствии со статусом сотрудника в системе и его правами; вести учёт рабочего времени; осуществлять централизованное управление охранно-пожарной составляющей системы, пожаротушением и доступом.

Указанной в п.1.1.8 настоящего документа:

Система предназначена для выполнения требований федерального законодательства по формированию открытости и общедоступности информационных ресурсов, содержащих информацию о деятельности учреждения, и обеспечивает доступ к таким ресурсам посредством размещения их в информационно-телекоммуникационных сетях, в частности - в сети «Интернет».

Указанной в п.1.1.9 настоящего документа:

Предназначена для автоматизации бухгалтерской система учета начислений и выплат стипендий студентам – «1С Зарплата и Кадры».

Указанной в п.1.1.10: настоящего документа

Предназначена для автоматизации, как планирования деятельности, так и контроля исполнения: составление рабочих учебных планов на базе

государственных стандартов, формирование, распределение и учет выполнения педагогической нагрузки, составление расписания и учет ежедневных замен, планирование и контроль исполнения мероприятий, учет успеваемости и посещаемости, планирование и проведение производственной практики, и многое другое. Позволяет учреждению: комплексно автоматизировать управление бизнеспроцессами, в частности работу приемной комиссии, осуществлять оперативное управление учебно-методическим процессом, студенческим контингентом; предоставить возможность накопления информации для анализа и дальнейшего принятия эффективных управленческих решений, качественно предоставлять услуги; обеспечить «прозрачность» управления как основным бизнеспроцессом (учебным процессом), так и вспомогательными процессами; предоставить учащимся и их родителям – основным клиентам учебного заведения – дополнительные информационные сервисы.

Указанной в п.1.1.11: настоящего документа

Система предназначена для обеспечения возможности хранения в базе данных специфичных для учреждений системы ПТО сведений: специальностей и квалификаций учащихся, форм, уровней обучения и специализаций групп, их кураторов и мастеров производственного обучения и пр.; в блоке "Нагрузка": возможно составление учебного плана по курсам и распределение нагрузки преподавателей на год; учет пропусков и опозданий учащихся (ввод и получение отчетов) отдельно для занятий по общеобразовательным предметам и предметам профессиональных циклов; система также предназначена для переноса информации в базу данных следующего учебного года с учетом вариантов окончания учебного года учащимися, а также сбора данных о различных категориях выпускников.

1.4 Состав и структура ПДн, обрабатываемых в ИСПДн

Состав и структура ПДн, обрабатываемых в ИСПДн приведены в таблице:

№ группы п/п	Наименование информации	Категория информации
1.	Фамилия, имя, отчество; пол; гражданство; дата и место рождения; изображение (фотография); паспортные данные; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные; сведения об образовании; индивидуальный номер налогоплательщика;	Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.1

№ группы п/п	Наименование информации	Категория информации
	страховой номер индивидуального лицевого счета (СНИЛС); сведения о воинском учете; сведения об инвалидности; иные персональные данные, сообщаемые студентами\абитуриентами в соответствии с требованиями законодательства и иных нормативных правовых актов.	
	Фамилия, имя, отчество; пол; гражданство; дата и место рождения; изображение (фотография); паспортные данные; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные; индивидуальный номер налогоплательщика; страховой номер индивидуального лицевого счета (СНИЛС); сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации; семейное положение, наличие детей, родственные связи; сведения о трудовой деятельности, в том числе наличие поощрений, награждений и (или) дисциплинарных взысканий; данные о регистрации брака; сведения о воинском учете; сведения об инвалидности; сведения об удержании алиментов; сведения о доходе с предыдущего места работы; иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.	Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.2
	Фамилия, имя, отчество; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные.	Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.3
	Фамилия, имя, отчество; паспортные данные; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные.	Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.4
	Фамилия, имя, отчество; пол; гражданство; дата и место рождения; паспортные данные; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные; индивидуальный номер налогоплательщика; страховой номер индивидуального лицевого счета (СНИЛС);	Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.5

№ группы п/п	Наименование информации	Категория информации
	сведения об инвалидности; сведения об удержании алиментов; сведения о доходе с предыдущего места работы; иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.	
	Фамилия, имя, отчество; пол; паспортные данные; контактные данные; индивидуальный номер налогоплательщика; страховой номер индивидуального лицевого счета (СНИЛС); иные персональные данные, предоставляемые работниками в соответствии с требованиями законодательства.	Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.6
	Фамилия, имя, отчество; пол; фото (видео); контактные данные; иные персональные данные, предоставляемые работниками, посетителями в соответствии с требованиями законодательства.	Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.7
	Фамилия, имя, отчество; пол; контактные данные; иные персональные данные, предоставляемые работниками или студентами в соответствии с требованиями законодательства.	Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.8
	Фамилия, имя, отчество; пол; гражданство; дата и место рождения; изображение (фотография); паспортные данные; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные; сведения об образовании; индивидуальный номер налогоплательщика; страховой номер индивидуального лицевого счета (СНИЛС); иные персональные данные, сообщаемые студентами\абитуриентами в соответствии с требованиями законодательства и иных нормативных правовых актов.	Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.9
	Фамилия, имя, отчество; пол; гражданство; дата и место рождения; изображение (фотография); паспортные данные; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные;	Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.10

№ группы п/п	Наименование информации	Категория информации
	сведения об образовании; индивидуальный номер налогоплательщика; страховой номер индивидуального лицевого счета (СНИЛС); сведения о воинском учете; сведения об инвалидности; иные персональные данные, сообщаемые студентами\абитуриентами в соответствии с требованиями законодательства и иных нормативных правовых актов.	
	Фамилия, имя, отчество; пол; гражданство; дата и место рождения; изображение (фотография); паспортные данные; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные; сведения об образовании; индивидуальный номер налогоплательщика; страховой номер индивидуального лицевого счета (СНИЛС); сведения о воинском учете; сведения об инвалидности; иные персональные данные, сообщаемые студентами\абитуриентами в соответствии с требованиями законодательства и иных нормативных правовых актов.	Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.11 настоящего документа
2.	Технологическая информация, не относящаяся к персональным данным, влияющая на целостность и устойчивость системы: – управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.); – технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа); – информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), о системе управления ресурсами или средствах доступа к этим системам управления; – информационные ресурсы (базы данных, файлы и другие), содержащие информацию об информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах; – служебные данные (метаданные), появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия в результате обработки информации.	Технологическая информация, для всех систем, указанных в п.1.1 настоящего документа

1.5 Процесс обработки информации (персональных данных) в ИСПДн

Под обработкой информации понимается любое действие (операция) или совокупность действий (операций) с данными, включая сбор, запись,

систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление или уничтожение данных.

Ввод данных в ИСПДн осуществляется сотрудниками Учреждения, назначенными соответствующим Приказом по Учреждению.

В ИСПДн указанных в п. 1.1.1, 1.1.9, 1.1.10, 1.1.11 производится обработка персональных данных субъектов ПДн, не являющихся сотрудниками оператора.

В ИСПДн указанных в п. 1.1.1…1.1.6 производится обработка персональных данных субъектов ПДн, являющихся сотрудниками оператора.

В ИСПДн указанных в п. 1.1.7, 1.1.8 производится обработка персональных данных субъектов ПДн, являющихся сотрудниками оператора и не являющимися сотрудниками оператора.

1.6 Состав и архитектура ИСПДн, интерфейсы и взаимосвязи компонентов

Технические средства, входящие в состав ИСПДн, перечисленные в п.1.1 настоящего документа, расположены по адресу: 197373, г Санкт-Петербург, пр-кт Авиаконструкторов, 28А.

Границей Контролируемой зоны (далее – КЗ) для ИСПДн перечисленных в п.1.1 настоящего документа, являются ограждающие конструкции здания основного учебного корпуса.

1.7 Структурные элементы ИСПДн

В состав ИСПДн, перечисленных в п.1.1 настоящего документа, входят следующие структурные элементы:

а) программно-технические средства обработки:

- общесистемное и специальное программное обеспечение, участвующее в обработке ПДн;
- средства и утилиты системы управления ресурсами ИСПДн;
- аппаратные средства обработки ПДн;

б) средства защиты ПДн:

- средства управления доступом пользователей (встроенные в ОС);
- средства обеспечения регистрации и учета действий с информацией (встроенные в ОС);
- средства, обеспечивающие целостность данных (встроенные в ОС);
- средства антивирусной защиты;

в) каналы информационного обмена и телекоммуникации;

г) помещения, в которых размещены компоненты ИСПДн, перечисленные в п 1.1 настоящего документа.

1.8 Описание внутренних и внешних (при наличии) групп пользователей

Объектами доступа в ИСПДн, указанных в п.1.1 настоящего документа, являются обрабатываемая информация, ПО и технические средства, средства защиты информации, используемые в ИСПДн.

Субъектами доступа являются пользователи, администраторы и администратор безопасности ИСПДн.

В ИСПДн, перечисленных в п.1.1 настоящего документа предусматривается наличие только постоянных пользователей из числа сотрудников Учреждения. Внешние пользователи в ИСПДн отсутствуют.

Режим обработки предусматривает следующие действия с защищаемой информации:

- сбор,
- запись,
- систематизация,
- уточнение (обновление, изменение),
- передача.

Обработка информации в ИСПДн производится следующим образом:

- ввод информации осуществляется пользователями вручную (с клавиатуры) в окне программы и\или интернет-браузера;
- хранение информации осуществляется с использованием ресурсов центра обработки данных для систем, указанных в п.1.1.1…1.1.6 а так же на серверах учреждения и, при необходимости на АРМ пользователей, съёмные носители информации используются;
- пользователи работают с информацией согласно назначенным им полномочиям.

1.9 Категории групп пользователей информации в ИСПДн

В ИСПДн, указанных в п.1.1 настоящего документа, обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа.

Персонал ИСПДн в общем случае подразделен на две категории.

Первая категория - обслуживающий персонал, включающий сотрудников, осуществляющих эксплуатацию и техническую поддержку обеспечения функционирования ИСПДн:

- администратор безопасности информации ИСПДн;
- администраторы ИСПДн.

В обязанности обслуживающего персонала входят:

- контроль состояния технических средств ИСПДн;

- регистрация пользователей в ИСПДн с присвоением каждому из них полномочий по доступу к информационным ресурсам ИСПДн;
- управление информационной безопасностью ИСПДн;
- учет средств защиты информации, используемых в ИСПДн;
- проведение регламентных и ремонтных работ и другие обязанности.

Вторая категория - эксплуатирующий персонал, который включает в себя пользователей автоматизированных рабочих мест ИСПДн.

Группа	Уровень доступа к ПДн	Разрешенные действия
Администраторы И администратор безопасности ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	Настройка, администрирование элементов и ПО ИСПДн
Пользователи ИСПДн	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ПДн.	Сбор, запись, систематизация, уточнение (обновление, изменение), передача

1.10 Описание внешних интерфейсов взаимодействия ИСПДн с пользователями, иными системами и сетями

ИСПДн являются распределенной многопользовательской информационной системой с разграничением прав доступа, и представляет собой автоматизированные рабочие место со следующим установленным программным обеспечением:

- операционная система Microsoft Windows;
- программное обеспечение для оборудования (драйверы и ПО устройств);
- веб-приложение (браузер);
- специализированное программное обеспечение рабочего места оператора или пользователя\абонента.

Взаимодействие ИСПДн, указанных в п.п.1.1.1…1.1.6 с центром обработки данных строится по принципу централизованной системы обработки данных, состоящей из центра обработки данных и АРМ пользователей(я) с коммутационным и прикладным оборудованием.

Взаимодействие ИСПДн, указанных в п.п.1.1.7…1.1.11 с серверами обеспечивается локальной вычислительной сетью с применением соответствующего коммуникационного и прикладного оборудования. Прикладное оборудование взаимодействует с АРМ пользователя посредством USB и Ethernet интерфейсов. Правила (допуски, права пользователей и др.) использования оборудования и программных средств

регламентируется в организационно-распорядительной и эксплуатационной документации.

2. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

На основе анализа исходных данных определена группа событий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к:

а) нарушению прав граждан;

б) возникновению рисков в оказании услуг для обладателя информации, оператора.

№	Виды риска (ущерба)	Возможные типовые негативные последствия
У1	Ущерб физическому лицу	Разглашение персональных данных граждан. Нарушение конфиденциальности (утечка) персональных данных. Унижение достоинства личности. Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.
У2	Риски в оказании услуг для обладателя информации, оператора	Нарушение законодательства Российской Федерации. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Дискредитация работников. Причинение имущественного ущерба. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением. Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени. Утечка конфиденциальной информации.

3. Описание возможных объектов воздействия угроз безопасности информации

На основе анализа исходных данных и результатов инвентаризации ИСПДн определены следующие группы информационных ресурсов и компоненты информационной системы, которые могут являться объектами воздействия:

а) информация (данные), содержащаяся в системах и сетях (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, сведения о событиях безопасности и др.);

б) программно-аппаратные средства обработки и хранения информации (в том числе автоматизированные рабочие места, серверы, средства отображения информации);

в) программные средства (в том числе системное и прикладное программное обеспечение);

г) машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию;

д) телекоммуникационное оборудование (в том числе программное обеспечение для управления телекоммуникационным оборудованием);

е) привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними.

Для определенных информационных ресурсов и компонентов систем и сетей определены виды воздействия на них, которые могут привести к негативным последствиям.

Основными видами таких воздействий являются:

а) утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);

б) несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;

в) отказ в обслуживании компонентов (нарушение доступности);

г) несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);

д) несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;

е) нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации.

ж) хищение ЗИ (месть, желание самореализоваться, получение преференций со стороны пользователя).

з) Подкуп, шантаж или меры физического воздействия для получения несанкционированного доступа со стороны злоумышленника.

и) Отказ в обслуживании пользователей (месть, профессиональная некомпетентность).

к) Невозможность оказания услуги (природные явления, техногенная катастрофа, отсутствие (недостаток) ресурсов).

Объекты воздействия угроз безопасности информации ИСПДн и видов воздействия на них

Негативные последствия	Объекты воздействия	Виды воздействия
Разглашение персональных данных граждан.	База данных информационной системы, содержащая конфиденциальную информацию	Несанкционированный доступ к персональным данным граждан, содержащихся в базе данных
	Автоматизированное рабочее место	Несанкционированный доступ к АРМ

Негативные последствия	Объекты воздействия	Виды воздействия
(У1)	(АРМ) пользователя	пользователя
		Утечка персональных данных граждан по визуальному каналу с удаленного АРМ пользователя.
	Линия связи между ЦОД и АРМ Учреждения	Перехват персональных данных граждан, передаваемых по линиям связи
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	Несанкционированный доступ к конфиденциальной информации, содержащейся в веб-приложении информационной системы
	Машинные носители информации, содержащие защищаемую информацию	Несанкционированный доступ к персональным данным граждан, содержащихся на машинных носителях информации.
	Телекоммуникационное оборудование информационной системы	Несанкционированный доступ к персональным данным граждан, передаваемым посредством телекоммуникационного оборудования
	Привилегированные и непривилегированные пользователи информационной системы	Хищение ЗИ: Месть, желание самореализоваться, получение преференций со стороны пользователя. Подкуп, шантаж или меры физического воздействия для получения несанкционированного доступа со стороны злоумышленника.
	Интерфейсы взаимодействия с внешними информационными системами	Несанкционированный доступ к интерфейсам взаимодействия с внешними информационными системами
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы виртуализации)	Несанкционированный доступ к программным средствам
Унижение достоинства личности. (У1)	База данных информационной системы, содержащая конфиденциальную информацию	НСД ЗИ
	Автоматизированное рабочее место пользователя	Утечка ЗИ
	Линия связи между ЦОД и АРМ Учреждения	Перехват ЗИ
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	НСД к ЗИ
	Машинные носители информации,	НСД к ЗИ

Негативные последствия	Объекты воздействия	Виды воздействия
	содержащие защищаемую информацию	
	Телекоммуникационное оборудование информационной системы	НСД к ЗИ
	Привилегированные и непривилегированные пользователи информационной системы	Хищение ЗИ: Месть, желание самореализоваться, получение преференций со стороны пользователя. Подкуп, шантаж или меры физического воздействия для получения несанкционированного доступа со стороны злоумышленника.
	Интерфейсы взаимодействия с внешними информационными системами	Утечка ЗИ
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы виртуализации)	НСД к ЗИ
Нарушение конфиденциальности (утечка) персональных данных. (У1)	База данных информационной системы, содержащая конфиденциальную информацию	НСД к защищаемой информации, системным, конфигурационным и иным служебным данным; Хищение (утечка) информации
	Автоматизированное рабочее место пользователя	НСД к АРМ; Хищение (утечка) информации; Утечка по визуальному каналу.
	Линия связи между ЦОД и АРМ Учреждения	Перехват ЗИ
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	НСД к ЗИ; Хищение ЗИ
	Машинные носители информации, содержащие защищаемую информацию	НСД к МНИ; Хищение МНИ; Утрата МНИ
	Телекоммуникационное оборудование информационной системы	Утечка (перехват) ЗИ, аутентифицирующей информации, системной, конфигурационной; Хищение ЗИ
	Привилегированные и непривилегированные пользователи информационной системы	Хищение ЗИ, аутентифицирующей информации, системной, конфигурационной
	Интерфейсы взаимодействия с внешними информационными	Утечка ЗИ, аутентифицирующей информации, системной,

Негативные последствия	Объекты воздействия	Виды воздействия
	системами	конфигурационной
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы виртуализации)	НСД к ЗИ; Утечка или хищение ЗИ, аутентифицирующей информации, системной, конфигурационной
Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. (У1)	База данных информационной системы, содержащая конфиденциальную информацию	Нарушение функционирования (работоспособности) базы данных информационной системы
	Линия связи между ЦОД и АРМ Учреждения	Нарушение функционирования (работоспособности)
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	Отказ в обслуживании
	Машинные носители информации, содержащие защищаемую информацию	Нарушение функционирования (работоспособности)
	Телекоммуникационное оборудование информационной системы	Отказ в обслуживании; Нарушение функционирования (работоспособности)
	Привилегированные и непривилегированные пользователи информационной системы	Отказ в обслуживании пользователей (месть, профессиональная некомпетентность). Невозможность оказания услуги по причине физической невозможности (болезнь, террористическая атака, природные явления, техногенная катастрофа, отсутствие (недостаток) ресурсов.
	Интерфейсы взаимодействия с внешними информационными системами	Нарушение функционирования (работоспособности)
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы виртуализации)	Нарушение функционирования (работоспособности)
Нарушение законодательства Российской Федерации. (У2)	База данных информационной системы, содержащая конфиденциальную информацию	Нарушение функционирования (работоспособности)
	Автоматизированное рабочее место пользователя	Нарушение функционирования (работоспособности)
	Линия связи между ЦОД и АРМ Учреждения	Нарушение функционирования (работоспособности)

Негативные последствия	Объекты воздействия	Виды воздействия
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	Отказ в обслуживании
	Машинные носители информации, содержащие защищаемую информацию	Нарушение функционирования (работоспособности)
	Телекоммуникационное оборудование информационной системы	Отказ в обслуживании
	Привилегированные и непривилегированные пользователи информационной системы	Отказ в обслуживании пользователей (месть, профессиональная некомпетентность). Невозможность услуги по причине физической невозможности (болезнь, террористическая атака, природные явления, техногенная катастрофа, отсутствие (недостаток) ресурсов.
	Интерфейсы взаимодействия с внешними информационными системами	Нарушение функционирования (работоспособности)
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы виртуализации)	Нарушение функционирования (работоспособности)
Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. (У2)	База данных информационной системы, содержащая конфиденциальную информацию	Нарушение функционирования (работоспособности) базы данных информационной системы
	Автоматизированное рабочее место пользователя	Нарушение функционирования (работоспособности)
	Линия связи между ЦОД и АРМ Учреждения	Нарушение функционирования (работоспособности)
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	Отказ в обслуживании
	Машинные носители информации, содержащие защищаемую информацию	Нарушение функционирования (работоспособности)
	Телекоммуникационное оборудование информационной системы	Отказ в обслуживании
	Привилегированные и непривилегированные пользователи информационной системы	Отказ в обслуживании пользователей (месть, профессиональная некомпетентность). Невозможность оказания услуги по причине физической невозможности (болезнь, террористическая атака,

Негативные последствия	Объекты воздействия	Виды воздействия
		природные явления, техногенная катастрофа, отсутствие (недостаток) ресурсов.
	Интерфейсы взаимодействия с внешними информационными системами	Нарушение функционирования (работоспособности)
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы виртуализации)	Нарушение функционирования (работоспособности)
Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).	Автоматизированное рабочее место пользователя	Нарушение функционирования (работоспособности)
	Линия связи между ЦОД и АРМ Учреждения	Нарушение функционирования (работоспособности)
	Машинные носители информации, содержащие защищаемую информацию	Нарушение функционирования (работоспособности)
	Телекоммуникационное оборудование информационной системы	Нарушение функционирования (работоспособности)
Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. (У2)	База данных информационной системы, содержащая конфиденциальную информацию	Нарушение функционирования (работоспособности)
	Автоматизированное рабочее место пользователя	Нарушение функционирования (работоспособности)
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	Нарушение функционирования (работоспособности)
	Машинные носители информации, содержащие защищаемую информацию	Нарушение функционирования (работоспособности)
	Телекоммуникационное оборудование информационной системы	Нарушение функционирования (работоспособности)
	Интерфейсы взаимодействия с внешними информационными системами	Нарушение функционирования (работоспособности)
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы	Нарушение функционирования (работоспособности)

Негативные последствия	Объекты воздействия	Виды воздействия
	виртуализации)	
Дискредитация работников. (У2)	База данных информационной системы, содержащая конфиденциальную информацию	НСД к ЗИ; Утечка ЗИ; Модификация ЗИ
	Автоматизированное рабочее место пользователя	НСД к ЗИ; Утечка ЗИ; Модификация ЗИ
	Линия связи между ЦОД и АРМ Учреждения	Утечка ЗИ
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	НСД к прикладному ПО; Утечка ЗИ; Модификация ЗИ
	Машинные носители информации, содержащие защищаемую информацию	НСД к МНИ; Утрата или хищение МНИ
	Телекоммуникационное оборудование информационной системы	НСД к ТКО; Утечка ЗИ
	Привилегированные и непривилегированные пользователи информационной системы	Хищение, модификация ЗИ: Месть, желание самореализоваться, получение преференций (со стороны пользователя). Подкуп, шантаж или меры физического воздействия для получения несанкционированного доступа (со стороны злоумышленника).
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы виртуализации)	НСД к ПО; Утечка ЗИ; Модификация ЗИ
Причинение имущественного ущерба. (У2)	Автоматизированное рабочее место пользователя	Нарушение функционирования (работоспособности) Утрата или хищение АРМ
	Линия связи между ЦОД и АРМ Учреждения	Нарушение функционирования (работоспособности)
	Машинные носители информации, содержащие защищаемую информацию	Нарушение функционирования (работоспособности); Утрата или хищение МНИ
	Телекоммуникационное оборудование информационной системы	Нарушение функционирования (работоспособности) Хищение ТКО
Невозможность решения задач	База данных информационной системы, содержащая	НСД к ЗИ; Модификация ЗИ;

Негативные последствия	Объекты воздействия	Виды воздействия
(реализации функций) или снижение эффективности решения задач (реализации функций). (У2)	конфиденциальную информацию	Нарушение функционирования (работоспособности)
	Автоматизированное рабочее место пользователя	НСД к АРМ; Модификация ЗИ; Нарушение функционирования (работоспособности)
	Линия связи между ЦОД и АРМ Учреждения	Отказ в обслуживании; Нарушение функционирования (работоспособности)
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	НСД к прикладному ПО; Модификация ЗИ; Отказ в обслуживании
	Машинные носители информации, содержащие защищаемую информацию	НСД к МНИ; Утрата или хищение МНИ; Нарушение функционирования (работоспособности)
	Телекоммуникационное оборудование информационной системы	НСД к ТКО; Отказ в обслуживании
	Привилегированные и непривилегированные пользователи информационной системы	Отказ в обслуживании пользователей (месть, профессиональная некомпетентность). Невозможность оказания услуги по причине физической невозможности (болезнь, террористическая атака, природные явления, техногенная катастрофа, отсутствие (недостаток) ресурсов.
	Интерфейсы взаимодействия с внешними информационными системами	Нарушение функционирования (работоспособности)
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы виртуализации)	НСД к ПО; Модификация ЗИ; Нарушение функционирования (работоспособности)
Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций).	База данных информационной системы, содержащая конфиденциальную информацию	НСД к ЗИ; Модификация ЗИ; Нарушение функционирования (работоспособности)
	Автоматизированное рабочее место пользователя	НСД к АРМ; Модификация ЗИ; Нарушение функционирования (работоспособности)
	Линия связи между ЦОД и АРМ	Нарушение функционирования

Негативные последствия	Объекты воздействия	Виды воздействия
(У2)	Учреждения	(работоспособности); Отказ в обслуживании
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	НСД к ПО; Модификация ЗИ; Отказ в обслуживании
	Машинные носители информации, содержащие защищаемую информацию	НСД к МНИ; Утрата или хищение МНИ; Нарушение функционирования (работоспособности)
	Телекоммуникационное оборудование информационной системы	НСД к ТКО; Отказ в обслуживании; Нарушение функционирования (работоспособности)
	Привилегированные и непривилегированные пользователи информационной системы	Отказ в обслуживании пользователей (месть, профессиональная некомпетентность). Невозможность оказания услуги по причине физической невозможности (болезнь, террористическая атака, природные явления, техногенная катастрофа, отсутствие (недостаток) ресурсов. Модификация ЗИ: Месть, желание самореализоваться, получение преференций (со стороны пользователя). Подкуп, шантаж или меры физического воздействия для получения несанкционированного доступа (со стороны злоумышленника).
	Интерфейсы взаимодействия с внешними информационными системами	Нарушение функционирования (работоспособности)
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы виртуализации)	НСД к ПО; Модификация ЗИ; Нарушение функционирования (работоспособности)
Использование веб-ресурсов для распространения и управления вредоносным программным	Автоматизированное рабочее место пользователя	НСД к АРМ
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	НСД к прикладному ПО

Негативные последствия	Объекты воздействия	Виды воздействия
обеспечением. (У2)	Машинные носители информации, содержащие защищаемую информацию	НСД к МНИ
	Телекоммуникационное оборудование информационной системы	НСД к ТКО
	Привилегированные и непривилегированные пользователи информационной системы	Распространение и управление ВПО: - месть, желание самореализоваться, получение преференций (со стороны пользователя); - подкуп, шантаж или меры физического воздействия для получения несанкционированного доступа (со стороны злоумышленника)
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы виртуализации)	НСД к ПО
Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени. (У2)	Автоматизированное рабочее место пользователя	НСД к АРМ
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	НСД к прикладному ПО
	Привилегированные и непривилегированные пользователи информационной системы	Рассылка информационных сообщений: - месть, желание самореализоваться, получение преференций (со стороны пользователя); - подкуп, шантаж или меры физического воздействия для получения несанкционированного доступа (со стороны злоумышленника)
Утечка конфиденциальной информации. (У2)	База данных информационной системы, содержащая конфиденциальную информацию	НСД к ЗИ; Утечка ЗИ
	Автоматизированное рабочее место пользователя	НСД к АРМ; Утечка ЗИ
	Линия связи между ЦОД и АРМ Учреждения	Утечка ЗИ
	Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию	НСД к ППО; Утечка ЗИ
	Машинные носители информации, содержащие защищаемую информацию	НСД к МНИ; Утрата или хищение МНИ

Негативные последствия	Объекты воздействия	Виды воздействия
	Телекоммуникационное оборудование информационной системы	НСД к ТКО; Утечка ЗИ
	Привилегированные и непривилегированные пользователи информационной системы	Хищение ЗИ: Месть, получение финансовой выгоды, получение преференций (со стороны пользователя). Подкуп, шантаж или меры физического воздействия для получения несанкционированного доступа со стороны злоумышленника.
	Интерфейсы взаимодействия с внешними информационными системами	Утечка ЗИ
	Программные средства (в том числе системное и прикладное программное обеспечение, включая серверы веб-приложений, системы управления базами данных, системы виртуализации)	НСД к ПО; Утечка ЗИ

4. Источники угроз безопасности информации

4.1. Характеристика нарушителей, которые могут являться источниками угроз безопасности информации, и возможные цели реализации ими угроз безопасности информации

На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации систем и сетей определялись виды актуальных нарушителей.

Оценке подлежали следующие основные виды нарушителей:

1) специальные службы иностранных государств;

2) террористические, экстремистские группировки;

3) преступные группы (криминальные структуры);

4) отдельные физические лица (хакеры);

5) конкурирующие организации;

6) разработчики программных, программно-аппаратных средств;

7) лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;

8) поставщики услуг связи, вычислительных услуг;

9) лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;

10) лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);

11) авторизованные пользователи систем и сетей;

12) системные администраторы и администраторы безопасности; бывшие (уволенные) работники (пользователи).

Возможные цели реализации угроз безопасности информации нарушителями:

№ вида	Виды нарушителя	Категория нарушителя	Возможные цели реализации угроз безопасности информации
1	Специальные службы иностранных государств	Внешний	Цели отсутствуют
2	Террористические, экстремистские группировки	Внешний	Цели отсутствуют
3	Преступные группы (криминальные структуры)	Внешний	Цели отсутствуют
4	Отдельные физические лица (хакеры)	Внешний	Желание самореализоваться.
5	Конкурирующие организации	Внешний	Цели отсутствуют
6	Разработчики программных, программно-аппаратных средств	Внутренний	Цели отсутствуют
7	Поставщики вычислительных услуг, услуг связи	Внутренний	Цели отсутствуют
8	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Непреднамеренные, неосторожные или неквалифицированные действия.
9	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Цели отсутствуют
10	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Непреднамеренные, неосторожные или неквалифицированные действия
11	Авторизованные пользователи систем и сетей	Внутренний	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.
12	Системные администраторы и администраторы безопасности	Внутренний	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия. Любопытство или желание самореализации (подтверждение статуса). Непреднамеренные, неосторожные или неквалифицированные действия.
13	Бывшие работники (пользователи)	Внешний	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия.

Нарушители признаются актуальными для систем и сетей, когда возможные цели реализации ими угроз безопасности информации могут привести к определенным для ИСПДн негативным последствиям и соответствующим рискам (видам ущерба).

В ходе оценки целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации была определена актуальность различных видов нарушителей.

Актуальные нарушители для ИСПДн, указанных в п.1.1 настоящего документа:

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу	Нанесение ущерба государству в социальной сфере деятельности	
Отдельные физические лица (хакеры)	–	+ (желание самореализоваться)	–	У2 Нарушение законодательства Российской Федерации. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Дискредитация работников. Причинение имущественного ущерба. Невозможность решения задач (реализации функций) или

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу	Нанесение ущерба государству в социальной сфере деятельности	
				снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени. Утечка конфиденциальной информации.
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	–	+ (непреднамеренные, неосторожные или неквалифицированные действия)	–	У2 Нарушение законодательства Российской Федерации. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу	Нанесение ущерба государству в социальной сфере деятельности	
				Причинение имущественного ущерба. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). Утечка конфиденциальной информации.
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т. д.)	–	+ (непреднамеренные, неосторожные или неквалифицированные действия)	–	У2 Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Утечка конфиденциальной информации.

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу	Нанесение ущерба государству в социальной сфере деятельности	
Авторизованные пользователи систем и сетей	+ (получение финансовой или иной материальной выгоды, месть за ранее совершенные действия, непреднамеренные, неосторожные или неквалифицированные действия)	+ (непреднамеренные, неосторожные или неквалифицированные действия)	–	У1 Разглашение персональных данных граждан. Унижение достоинства личности. Нарушение конфиденциальности (утечка) персональных данных. Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. У2 Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.
Системные администраторы и администраторы безопасности	+ (получение финансовой или иной материальной выгоды, месть за ранее совершенные действия,	+ (получение финансовой или иной материальной выгоды, любопытство или желание самореализации	–	У1 Разглашение персональных данных граждан. Нарушение конфиденциальности (утечка) персональных данных. Унижение достоинства личности. Нарушение прав гражданина, закрепленных в Конституции

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу	Нанесение ущерба государству в социальной сфере деятельности	
	любопытство)	(подтверждение статуса), непреднамеренные, неосторожные или неквалифицированные действия)		Российской Федерации и федеральных законах. У2 Нарушение законодательства Российской Федерации. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Причинение имущественного ущерба. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций).

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу	Нанесение ущерба государству в социальной сфере деятельности	
				Публикация недостоверной информации на веб-ресурсах организации. Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением. Утечка конфиденциальной информации.
Бывшие (уволенные) работники (пользователи)	+ (получение финансовой или иной материальной выгоды, месть за ранее совершенные действия)	+ (месть за ранее совершенные действия)	–	У1 Разглашение персональных данных граждан. Нарушение конфиденциальности (утечка) персональных данных. Унижение достоинства личности. Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. У2 Причинение имущественного ущерба.

4.2 Описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей

Актуальные нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителей по реализации угроз безопасности информации для систем и сетей.

В зависимости от уровня возможностей актуальные нарушители подразделяются на нарушителей, обладающих:

– базовыми возможностями по реализации угроз безопасности информации (Н1);

– базовыми повышенными возможностями по реализации угроз безопасности информации (Н2).

Для одной системы или сети актуальными могут являться нарушители, имеющие разные уровни возможностей.

Уровни возможностей актуальных нарушителей по реализации угроз безопасности информации для ИСПДн, указанных в п.1.1 настоящего документа

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Н1	Нарушитель, обладающий базовыми возможностями	Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. **Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов**	Физическое лицо (хакер) Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.) Авторизованные пользователи систем и сетей Бывшие работники (пользователи)
Н2	Нарушитель, обладающий базовыми повышенными возможностями	Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ Системные администраторы и администраторы

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
		повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. **Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей**	безопасности

4.3 Категории актуальных нарушителей, которые могут являться источниками угроз безопасности информации

Для актуальных нарушителей определены их категории в зависимости от имеющихся прав и условий по доступу к ИСПДн, указанных в п.1.1 настоящего документа, обусловленных архитектурой и условиями функционирования ИСПДн, а также от установленных возможностей нарушителей. При этом нарушители подразделяются на две категории:

- внешние нарушители – нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам ИСПДн, требующим авторизации;
- внутренние нарушители – нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам ИСПДн.

Внутренние нарушители первоначально могут иметь разный уровень прав доступа к информационным ресурсам и компонентам ИСПДн (исполнение обязанностей на автоматизированном рабочем месте, администрирование систем и сетей).

К внутренним нарушителям относятся пользователи, имеющие как непривилегированные (пользовательские), так и привилегированные (административные) права доступа к информационным ресурсам и компонентам ИСПДн.

Внешние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых.

Внутренние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых или непреднамеренно (непреднамеренные угрозы безопасности информации) без использования программных, программно-аппаратных средств.

Виды актуальных нарушителей при реализации угроз безопасности информации ИСПДн:

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	У1:	Авторизованные пользователи систем и	Внутренний	Н1

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
	Разглашение персональных данных граждан; нарушение конфиденциальности (утечка) персональных данных; унижение достоинства личности; нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.	сетей		
		Системные администраторы и администраторы безопасности	Внутренний	Н2
		Бывшие работники (пользователи)	Внешний	Н1
2	У2: Нарушение законодательства Российской Федерации; необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств); необходимость дополнительных (незапланированных) затрат на восстановление деятельности; дискредитация работников; причинение имущественного ущерба; невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций); использование веб-ресурсов для распространения и управления вредоносным программным обеспечением; рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени; утечка конфиденциальной информации.	Отдельные физические лица (хакеры)	Внешний	Н1
		Системные администраторы и администраторы безопасности	Внутренний	Н2
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.)	Внутренний	Н1
		Авторизованные пользователи систем и сетей	Внутренний	Н1
		Бывшие работники (пользователи)	Внешний	Н1

5. Способы реализации (возникновения) угроз безопасности информации в ИСПДн

5.1 Способы реализации угроз безопасности

Актуальные способы реализации (возникновения) угроз безопасности информации систем и сетей определяются на основании исходных данных, а также возможностей нарушителей.

При этом, основными способами реализации (возникновения) угроз безопасности информации являются:

1) использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей);

2) внедрение вредоносного программного обеспечения;

3) использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств;

4) установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;

5) формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;

6) инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;

7) нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);

8) ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

Способы реализации угроз безопасности информации определены применительно к объектам воздействия, определенным раннее.

Способы являются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз безопасности и имеются или созданы условия, при которых такая возможность может быть реализована в отношении объектов воздействия.

5.2 Описание интерфейсов объектов воздействия, используемых нарушителем

Условием, позволяющим актуальным нарушителям использовать способы реализации угроз безопасности информации, является наличие у них возможности доступа к следующим типам интерфейсов объектов воздействия:

1) внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);

2) внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами ИСПДн, имеющими внешние сетевые интерфейсы (проводные, беспроводные);

3) интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);

4) интерфейсы для использования съемных машинных носителей информации и периферийного оборудования;

5) интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов ИСПДн;

6) возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам ИСПДн.

Наличие указанных интерфейсов определяется архитектурой, составом и условиями функционирования ИСПДн, группами пользователей, их типами доступа и уровнями полномочий.

В ходе анализа определены как логические, так и физические интерфейсы объектов воздействия, в том числе требующие физического доступа к ним.

Интерфейсы определены на аппаратном, системном и прикладном уровнях ИСПДн , а также для телекоммуникационного оборудования. Возможность их использования на указанных уровнях определяется возможностями актуальных нарушителей.

Определение актуальных способов реализации угроз безопасности информации ИСПДн и соответствующие им виды нарушителей и их возможности

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Отдельные физические лица (хакеры) (Н1)	Внешний	АРМ пользователя: НСД к АРМ; Модификация ЗИ; Нарушение функционирования (работоспособности)	Сетевой интерфейс	Внедрение вредоносного программного обеспечения. Использование недекларированных возможностей программного обеспечения.
				Сменные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя. Использование ошибок настройки системы контроля действий пользователя.
			Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию: НСД к прикладному ПО; Модификация ЗИ; Отказ в обслуживании	Веб-интерфейс пользователя, администратора ППО информационной системы	Использование уязвимостей кода программного обеспечения веб-приложения. Использование недекларированных возможностей программного обеспечения.
			Интерфейсы взаимодействия с внешними информационными системами: Нарушение функционирования	Интерфейс ввода-вывода информации	Использование уязвимостей кода ППО. Использование недекларированных возможностей ППО.

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			(работоспособности)		
			Программные средства (в том числе прикладное программное обеспечение): НСД к ПО; Модификация ЗИ; Нарушение функционирования (работоспособности)	Пользовательский интерфейс прикладного ПО	Использование уязвимостей кода ПО. Внедрение вредоносного программного обеспечения.
2	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ (Н2)	Внутренний	АРМ пользователя: НСД к АРМ; Модификация данных	Сетевой интерфейс	Внедрение вредоносного программного обеспечения. Использование недекларированных возможностей программного обеспечения.
				Интерфейс ввода-вывода информации	Физический доступ к оборудованию.
				Сменные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя. Использование ошибок настройки системы контроля действий пользователя.

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			АРМ пользователя: Нарушение функционирования (работоспособности)	Физический доступ	Непреднамеренные, неосторожные или неквалифицированные действия.
			Линия связи между сервером основного центра обработки данных и АРМ пользователя: Отказ в обслуживании; Нарушение функционирования (работоспособности)	Канал передачи данных между сервером основного центра обработки данных и АРМ пользователя	Физический доступ к ТКО, кабелю линии связи.
			Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию: НСД к ППО; Модификация данных; Отказ в обслуживании; Нарушение функционирования (работоспособности)	Веб-интерфейс пользователя, администратора ППО информационной системы	Использование уязвимостей кода программного обеспечения веб-приложения. Использование недекларированных возможностей программного обеспечения.
			Машинные носители информации, содержащие защищаемую информацию: Хищение МНИ;	Физический доступ	Непосредственный доступ к МНИ

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			Утрата МНИ; Нарушение функционирования (работоспособности)		
			Телекоммуникационное оборудование информационной системы: НСД к ТКО; Отказ в обслуживании; Нарушение функционирования (работоспособности)	Физический доступ	Непосредственный доступ к ТКО
			Программные средства (в том числе прикладное программное обеспечение): НСД к ПО; Нарушение функционирования (работоспособности)	Пользовательский интерфейс прикладного ПО	Использование уязвимостей кода ПО. Внедрение вредоносного программного обеспечения.
3	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т. д.) (Н1)	Внутренний	Линия связи между сервером основного центра обработки данных и АРМ пользователя: Нарушение функционирования (работоспособности)	Физический доступ к ТКО, кабелю линии связи.	Непреднамеренные, неосторожные или неквалифицированные действия.
			Сменные машинные носители информации, содержащие защищаемую информацию: Нарушение функционирования	Физический доступ	Непреднамеренные, неосторожные или неквалифицированные действия.

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			(работоспособности)		
			Телекоммуникационное оборудование информационной системы: Нарушение функционирования (работоспособности)	Физический доступ	Непреднамеренные, неосторожные или неквалифицированные действия.
			База данных информационной системы, содержащая конфиденциальную информацию: Хищение (утечка) информации; Нарушение функционирования (работоспособности)	Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование режима доступа, предусмотренного для авторизованного пользователя.
4	Авторизованные пользователи систем и сетей (H1)	Внутренний	АРМ пользователя: Хищение (утечка) информации; Нарушение функционирования (работоспособности)	Сетевой интерфейс	Внедрение вредоносного программного обеспечения. Использование недекларированных возможностей программного обеспечения.
				Сменные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя. Использование ошибок настройки системы контроля действий пользователя.

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
				Интерфейс ввода-вывода	Внедрение вредоносного программного обеспечения. Непреднамеренные, неосторожные или неквалифицированные действия.
			Линия связи между сервером основного центра обработки данных и АРМ пользователя: Перехват ЗИ Нарушение функционирования (работоспособности)	Физический доступ к ТКО, кабелю линии связи.	Непреднамеренные, неосторожные или неквалифицированные действия. Месть за ранее совершенные действия.
			Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию: Хищение (утечка) информации Нарушение функционирования (работоспособности)	Веб-интерфейс пользователя, администратора ППО информационной системы	Использование режима доступа, предусмотренного для авторизованного пользователя и системного администратора. Использование уязвимостей кода программного обеспечения веб-приложения. Использование недекларированных возможностей программного обеспечения.
			Машинные носители информации, содержащие защищаемую информацию: Хищение МНИ;	Физический доступ	Непреднамеренные, неосторожные или неквалифицированные действия. Месть за ранее совершенные действия.

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			Утрата МНИ; Нарушение функционирования (работоспособности)		
			Телекоммуникационное оборудование информационной системы: Хищение (утечка) информации; Нарушение функционирования (работоспособности)	Физический доступ	Непреднамеренные, неосторожные или неквалифицированные действия. Месть за ранее совершенные действия.
			Программные средства (в том числе прикладное программное обеспечение) Хищение (утечка) информации Нарушение функционирования (работоспособности)	Пользовательский интерфейс прикладного программного обеспечения	Использование уязвимостей кода ПО. Внедрение вредоносного программного обеспечения.
			База данных информационной системы, содержащая конфиденциальную информацию: НСД к БД; Модификация данных; Нарушение функционирования (работоспособности)	Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование режима доступа, предусмотренного для системного администратора
5	Системные администраторы и администраторы	Внутренний	АРМ пользователя: НСД к АРМ;	Сетевой интерфейс	Использование режима доступа, предусмотренного для системного администратора

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
	безопасности (Н2)		Модификация данных	Интерфейс ввода-вывода информации	Использование режима доступа, предусмотренного для системного администратора
				Сменные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя. Использование ошибок настройки системы контроля действий пользователя.
			Линия связи между сервером основного центра обработки данных и АРМ пользователя: Отказ в обслуживании; Нарушение функционирования (работоспособности)	Канал передачи данных между сервером основного центра обработки данных и АРМ пользователя	Физический доступ к ТКО, кабелю линии связи.
			Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию: НСД к ППО; Модификация данных; Отказ в обслуживании; Нарушение функционирования (работоспособности)	Веб-интерфейс пользователя, администратора ППО информационной системы	Использование уязвимостей кода программного обеспечения веб-приложения. Использование недекларированных возможностей программного обеспечения. Использование ВПО.
			Машинные носители информации, содержащие защищаемую	Физический доступ	Нарушение функционирования в результате:

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			информацию: НСД к МНИ (серверным); Модификация данных; Хищение МНИ; Нарушение функционирования (работоспособности)		непреднамеренных, неосторожных или неквалифицированных действий; осуществления мести за ранее совершенные действия. НСД. Хищение МНИ.
			Телекоммуникационное оборудование информационной системы: НСД к ТКО; Отказ в обслуживании; Нарушение функционирования (работоспособности)	Физический доступ к оборудованию.	Нарушение функционирования в результате: непреднамеренных, неосторожных или неквалифицированных действий; осуществления мести за ранее совершенные действия. Хищение ТКО.
			Интерфейсы взаимодействия с внешними информационными системами: Нарушение функционирования (работоспособности)	Сетевой интерфейс	Использование режима доступа, предусмотренного для системного администратора. Использование уязвимостей кода ППО. Использование недекларированных возможностей ППО.
			Программные средства (в том числе системное и прикладное программное обеспечение): НСД к ПО;	Пользовательский интерфейс прикладного программного обеспечения	Использование режима доступа, предусмотренного для системного администратора. Использование уязвимостей кода

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			Нарушение функционирования (работоспособности)		системного ПО. Внедрение вредоносного программного обеспечения.
			База данных информационной системы, содержащая конфиденциальную информацию: Хищение (утечка) информации; Нарушение функционирования (работоспособности)	Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование режима доступа, предусмотренного для авторизованного пользователя.
6	Бывшие (уволенные) работники (пользователи) (H1)	Внешний	АРМ пользователя: Хищение (утечка) информации; Нарушение функционирования (работоспособности)	Сетевой интерфейс	Внедрение вредоносного программного обеспечения. Использование недекларированных возможностей программного обеспечения.
				Сменные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя. Использование ошибок настройки системы контроля действий пользователя.
				Интерфейс ввода-вывода информации	Внедрение вредоносного программного обеспечения. Непреднамеренные, неосторожные или неквалифицированные действия.

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			Линия связи между сервером основного центра обработки данных и АРМ пользователя: Перехват ЗИ; Нарушение функционирования (работоспособности)	Физический доступ к ТКО, кабелю линии связи.	Непреднамеренные, неосторожные или неквалифицированные действия. Месть за ранее совершенные действия.
			Веб-приложение информационной системы, обрабатывающей конфиденциальную информацию: Хищение (утечка) информации; Нарушение функционирования (работоспособности)	Веб-интерфейс пользователя, администратора ППО информационной системы	Использование режима доступа, предусмотренного для авторизованного пользователя. Использование уязвимостей кода программного обеспечения веб-приложения. Использование недекларированных возможностей программного обеспечения.
			Машинные носители информации, содержащие защищаемую информацию: Хищение МНИ; Утрата МНИ; Нарушение функционирования (работоспособности)	Физический доступ	Непреднамеренные, неосторожные или неквалифицированные действия. Месть за ранее совершенные действия.
			Телекоммуникационное оборудование информационной	Физический доступ	Непреднамеренные, неосторожные или неквалифицированные действия.

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			системы: Хищение (утечка) информации; Нарушение функционирования (работоспособности)		Месть за ранее совершенные действия.
			Программные средства (в том числе прикладное программное обеспечение): Хищение (утечка) информации; Нарушение функционирования (работоспособности)	Интерфейс прикладного программного обеспечения	Использование уязвимостей кода прикладного ПО. Внедрение вредоносного программного обеспечения.

6 Актуальные угрозы безопасности информации

6.1 Перечень возможных угроз безопасности

Возможные для ИСПДн угрозы безопасности информации, к которым относятся осуществляемые нарушителем воздействия на информационные ресурсы и компоненты ИСПДн (объекты воздействия), в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования ИСПДн определяются на основе анализа исходных данных.

Возможность угрозы безопасности информации определялась из условия, что имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям.

Перечень возможных для ИСПДн угроз безопасности информации

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
УБИ.004	Угроза аппаратного сброса пароля BIOS	Внутренний нарушитель с низким потенциалом H1, H2	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Использование уязвимостей системных (материнских) плат – наличие механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Физический доступ к системному блоку АРМ.	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.006	Угроза внедрения кода или данных	Внешний нарушитель с низким потенциалом H1	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	Внедрение вредоносного программного обеспечения Использование уязвимостей кода системного ПО.	Нарушение конфиденциальности (утечка) персональных данных. Нарушение законодательства Российской Федерации. Невозможность решения задач (реализации функций) или снижение эффективности решения задач

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
					(реализации функций).
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя	Доступ к АРМ пользователя через консоль.	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Внутренний нарушитель с низким потенциалом H1, H2	Микропрограммное обеспечение BIOS/UEFI	Использование слабостей технологий контроля за обновлением программного обеспечения BIOS/UEFI	Нарушение конфиденциальности (утечка) персональных данных. Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
					Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Внутренний нарушитель с низким потенциалом H1, H2	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, метаданные, объекты файловой системы, реестр	Использование слабостей мер контроля целостности конфигурационных файлов или библиотек, используемых приложениями.	Нарушение конфиденциальности (утечка) персональных данных. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности Невозможность решения задач (реализации функций) или снижение эффективности решения задач

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
					(реализации функций).
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Внутренний нарушитель с низким потенциалом H1, H2	Микропрограммное обеспечение BIOS/UEFI	Использование уязвимостей программного обеспечения BIOS/UEFI	Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	Использование уязвимостей программ, распределяющих вычислительные ресурсы между задачами.	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Внутренний нарушитель с низким потенциалом H1, H2	Объекты файловой системы	Доступ через консоль АРМ, через локальную вычислительную сеть организации	Нарушение конфиденциальности (утечка) персональных данных.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		Внешний нарушитель с низким потенциалом H1			
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Внешний нарушитель с низким потенциалом H1	Прикладное программное обеспечение, сетевое программное обеспечение	Использование слабостей мер защиты cookies-файлов.	Нарушение конфиденциальности (утечка) персональных данных. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.018	Угроза загрузки нештатной операционной системы	Внутренний нарушитель с низким потенциалом H1, H2	Микропрограммное обеспечение BIOS/UEFI	Физический доступ к АРМ. Использование слабостей технологий разграничения доступа к управлению BIOS/UEFI	Нарушение конфиденциальности (утечка) персональных данных. Нарушение прав

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
					гражданина, закрепленных в Конституции Российской Федерации и федеральных законах Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.019	Угроза заражения DNS-кеша	Внешний нарушитель с низким потенциалом H1	Сетевой узел, сетевое программное обеспечение, сетевой трафик	Использование слабостей механизмов проверки подлинности субъектов сетевого взаимодействия, а также уязвимостей DNS-сервера.	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.022	Угроза избыточного выделения оперативной памяти	Внутренний нарушитель с низким потенциалом H1, H2	Аппаратное обеспечение, системное программное обеспечение, сетевое программное обеспечение	Внедрение вредоносного программного обеспечения.	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		Внешний нарушитель с низким потенциалом H1			
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы	Внутренний нарушитель с низким потенциалом H1, H2	Информационная система, сервер, рабочая станция, виртуальная машина, системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	Физический доступ к АРМ, серверу, ТКО, машинным носителям информации, содержащим защищаемую информацию, линиям связи между сервером основного центра обработки данных и АРМ	Нарушение конфиденциальности (утечка) персональных данных. Нарушение законодательства Российской Федерации. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внутренний нарушитель с низким	Системное программное обеспечение,	Внедрение вредоносного программного обеспечения,	Дискредитация работников.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		потенциалом H1, H2	прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение	установка аппаратных закладок Установка аппаратных закладок	
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение	Использование уязвимостей мер разграничения доступа к защищаемой информации, слабости фильтрации входных данных	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внутренний нарушитель с низким потенциалом H1, H2	Средства защиты информации, системное программное обеспечение, сетевое программное обеспечение, микропрограммное	Использование уязвимостей устройств идентификации и аутентификации	Нарушение конфиденциальности (утечка) персональных данных. Унижение достоинства

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
			обеспечение, программно-аппаратные средства со встроенными функциями защиты		личности. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	Использование слабостей мер разграничения доступа к программам и файлам	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное	Использование слабостей протоколов (заложенных в них алгоритмов), ошибок, допущенных в ходе реализации протоколов, или	Нарушение конфиденциальности (утечка) персональных данных.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		H1, H2 Внешний нарушитель с низким потенциалом H1	обеспечение, сетевой трафик	уязвимостей, внедряемых автоматизированных средств проектирования/разработки	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Нарушение законодательства Российской Федерации
УБИ.041	Угроза межсайтового скриптинга	Внешний нарушитель с низким потенциалом H1	Сетевой узел, сетевое программное обеспечение	Внедрение вредоносного программного обеспечения.	Утечка конфиденциальной информации. Нарушение законодательства Российской Федерации Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Внутренний нарушитель с низким потенциалом H1, H2	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Использование слабостей технологий разграничения доступа к BIOS/UEFI, его функций администрирования и обновления, со стороны операционной системы или каналов связи.	Утечка конфиденциальной информации. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.049	Угроза нарушения целостности данных кеша	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким	Сетевое программное обеспечение	Использование слабостей в механизме контроля целостности данных в кеше.	Нарушение законодательства Российской Федерации. Невозможность решения задач (реализации функций) или снижение эффективности решения задач

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		потенциалом H1			(реализации функций).
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Внутренний нарушитель с низким потенциалом H1, H2	Рабочая станция, носитель информации, системное программное обеспечение, метаданные, объекты файловой системы, реестр	Использование ошибок в реализации программно-аппаратных компонентов компьютера, связанных с обеспечением питания.	Нарушение законодательства Российской Федерации. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.053	Угроза невозможности управления правами пользователей BIOS	Внутренний нарушитель с низким потенциалом H1, H2	Микропрограммное обеспечение BIOS/UEFI	Физический доступ к терминалу и, при необходимости, к системному блоку компьютера.	Нарушение конфиденциальности (утечка) персональных данных. Нарушение законодательства Российской Федерации.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
					Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Внешний нарушитель с низким потенциалом H1	Сетевое программное обеспечение	Использование слабостями механизма контроля доступа к настройкам браузера	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Внутренний нарушитель с низким потенциалом H1, H2	Аппаратное обеспечение, носители информации, объекты файловой системы	Использование уязвимостей средств контроля доступа, ошибок в параметрах конфигурации данных средств или отсутствия указанных средств	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.069	Угроза неправомерных действий в каналах связи	Внешний нарушитель с низким потенциалом H1	Сетевой трафик	Использование слабостей сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных	Нарушение конфиденциальности (утечка) персональных данных. Нарушение прав

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
					гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Машинный носитель информации	Использование слабостей механизма удаления информации с машинных носителей	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Внутренний нарушитель с низким потенциалом H1, H2	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Использование слабостей мер по разграничению доступа к управлению механизмом защиты BIOS/UEFI от записи, а также уязвимостей механизма обновления BIOS/UEFI, приводящих к переполнению буфера	Нарушение конфиденциальности (утечка) персональных данных. Нарушение законодательства Российской

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
					Федерации. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр, машинные носители информации	Доступ через локальную вычислительную сеть организации Физический доступ к машинным носителям информации	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	Внутренний нарушитель с низким потенциалом	Сетевое программное обеспечение, сетевой трафик, виртуальные устройства	Использование слабостей мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении	Нарушение конфиденциальности (утечка) персональных данных.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		H1, H2 Внешний нарушитель с низким потенциалом H1		сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных).	
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр	Использование слабостей мер разграничения доступа к информации аутентификации.	Нарушение конфиденциальности (утечка) персональных данных. Нарушение законодательства Российской Федерации. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Внутренний нарушитель с низким	Аппаратное обеспечение, микропрограммное	Использование потенциально опасных возможностей BIOS/UEFI	Нарушение конфиденциальности (утечка) персональных

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		потенциалом H1, H2	обеспечение BIOS/UEFI		данных. Нарушение законодательства Российской Федерации. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом	Объекты файловой системы, машинный носитель информации	Использование слабостей механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне.	Разглашение персональных данных граждан.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		H1			
УБИ.089	Угроза несанкционированного редактирования реестра	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Системное программное обеспечение, использующее реестр, реестр	Использование слабостей механизма контроля доступа, заключающимися в присвоении реализующим его программам слишком высоких привилегий при работе с реестром.	Нарушение конфиденциальности (утечка) персональных данных. Нарушение законодательства Российской Федерации. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Внутренний нарушитель с низким потенциалом H1, H2	Системное программное обеспечение	Использование слабостей механизмов разграничения доступа к защищаемой информации.	Нарушение конфиденциальности (утечка) персональных данных. Нарушение

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		Внешний нарушитель с низким потенциалом H1			законодательства Российской Федерации. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Метаданные, объекты файловой системы, реестр	Использование уязвимостей в программном обеспечении, реализующих меры по обеспечению доступности защищаемой информации в системе	Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.
УБИ.093	Угроза несанкционированного управления буфером	Внутренний нарушитель с	Системное программное	Использование слабостей в механизме разграничения доступа к	Нарушение конфиденциальности

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	буферу обмена, а также слабостей в механизмах проверки вводимых данных.	(утечка) персональных данных. Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Внешний нарушитель с низким потенциалом H1	Сетевой узел, сетевое программное обеспечение, сетевой трафик	Использование уязвимостей и ошибок конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе.	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.099	Угроза обнаружения хостов	Внешний нарушитель с	Сетевой узел, сетевое программное	Использование слабостей механизмов сетевого	Нарушение

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		низким потенциалом H1	обеспечение, сетевой трафик	взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой систем	конфиденциальности Нарушение конфиденциальности (утечка) персональных данных.
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Системное программное обеспечение, сетевое программное обеспечение	Использование некорректных значений параметров конфигурации средств аутентификации и/или отсутствием контроля входных данных	Нарушение конфиденциальности (утечка) персональных данных. Дискредитация работников. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.103	Угроза определения типов объектов защиты	Внешний нарушитель с низким	Сетевой узел, сетевое программное обеспечение, сетевой	Использование ошибок в параметрах конфигурации средств межсетевого экранирования, а также отсутствия	Нарушение конфиденциальности (утечка) персональных

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		потенциалом Н1	трафик	механизмов контроля входных и выходных данных	данных.
УБИ.104	Угроза определения топологии вычислительной сети	Внешний нарушитель с низким потенциалом Н1	Сетевой узел, сетевое программное обеспечение, сетевой трафик	Использование слабостей механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями средств межсетевого экранирования (алгоритма работы и конфигурации правил фильтрации сетевого трафика)	Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени.
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внутренний нарушитель с низким потенциалом Н1, Н2 Внешний нарушитель с низким потенциалом Н1	Системное программное обеспечение, аппаратное обеспечение	Использование свойств оперативной памяти обнулять своё состояние при выключении и перезагрузке. Физический доступ к АРМ.	Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Внутренний нарушитель с низким потенциалом Н1, Н2 Внешний нарушитель с низким потенциалом Н1	Системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	Установка и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др.	Утечка конфиденциальной информации.
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Внешний нарушитель с низким потенциалом Н1	Сетевой узел, сетевой трафик	Использование слабостей механизмов сетевого взаимодействия, предоставляющими сторонним пользователям открытые данные о дискредитируемой системе, а также ошибки конфигурации сетевого программного обеспечения	Утечка конфиденциальной информации.
УБИ.121	Угроза повреждения системного реестра	Внутренний нарушитель с низким потенциалом Н1, Н2	Объекты файловой системы, реестр	Использование слабостей мер контроля доступа к файлам, содержащим данные реестра, мер резервирования и контроля целостности таких файлов, а также мер восстановления работоспособности реестра из-за	Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		Внешний нарушитель с низким потенциалом H1		сбоев в работе операционной системы.	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.123	Угроза подбора пароля BIOS	Внутренний нарушитель с низким потенциалом H1, H2	Микропрограммное обеспечение BIOS/UEFI	Физический доступ к АРМ. Использование слабостей механизма аутентификации, реализуемого в консолях BIOS/UEFI.	Нарушение конфиденциальности (утечка) персональных данных. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.124	Угроза подделки записей журнала регистрации событий	Внутренний нарушитель с низким потенциалом H1, H2	Системное программное обеспечение	Использование недостаточности мер по разграничению доступа к журналу регистрации событий безопасности.	Дискредитация работников.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		Внешний нарушитель с низким потенциалом H1			
УБИ.128	Угроза подмены доверенного пользователя	Внешний нарушитель с низким потенциалом H1	Сетевой узел, сетевое программное обеспечение	Использование слабостей технологий сетевого взаимодействия, зачастую не позволяющие выполнить проверку подлинности источника/получателя информации.	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Внутренний нарушитель с низким потенциалом H1, H2	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Физический доступ к АРМ. Использование недостаточности мер разграничения доступа и контроля целостности резервных копий программного обеспечения BIOS/UEFI.	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Внешний нарушитель с низким потенциалом H1	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	Использование слабостей технологий сетевого взаимодействия, зачастую не позволяющие выполнить проверку подлинности содержимого электронного сообщения.	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.140	Угроза приведения системы в состояние	Внутренний	Информационная	Использование слабостей сетевых	Невозможность

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
	«отказ в обслуживании»	нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, телекоммуникационное устройство	технологий, связанных с ограниченностью скорости обработки потоков сетевых запросов, и недостаточностью мер контроля за управлением соединениями и ошибками реализации сетевых протоколов	решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.144	Угроза программного сброса пароля BIOS	Внутренний нарушитель с низким потенциалом H1, H2	Микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение	Физический доступ к АРМ для несанкционированного доступа к настройкам BIOS/UEFI после перезагрузки компьютера путём ввода «пустого» пароля. Использование слабостей мер разграничения доступа в операционной системе к функции сброса пароля BIOS/UEFI.	Нарушение конфиденциальности (утечка) персональных данных. Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Внутренний нарушитель с	Системное программное	Внедрение вредоносного программного обеспечения	Нарушение законодательства

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	обеспечение, прикладное программное обеспечение, сетевое программное обеспечение		Российской Федерации. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализаций функций).
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL.	Внешний нарушитель с низким потенциалом H1	Сетевое программное обеспечение, сетевой узел	Использование недостаточности мер по обеспечению конфиденциальности информации, реализованных в WSDL-сервисах, предоставляющих подробные сведения о портах, службах и соединениях, доступных пользователям.	Утечка конфиденциальной информации.
УБИ.152	Угроза удаления аутентификационной информации	Внутренний нарушитель с низким потенциалом H1, H2 Внешний	Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя	Использование слабостей политики разграничения доступа к аутентификационной информации и средствам работы с учётными записями пользователей.	Утечка конфиденциальной информации. Нарушение прав гражданина, закрепленных в

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		нарушитель с низким потенциалом H1			Конституции Российской Федерации и федеральных законах Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение	Использование слабостей мер межсетевого экранирования дискредитируемой информационной системы, мер контроля подлинности сетевых запросов на сторонних серверах, а также слабостями модели взаимодействия открытых систем.	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.155	Угроза утраты вычислительных ресурсов	Внутренний нарушитель с	Информационная система, сетевой узел,	Использование слабостей механизма контроля за распределением	Рассылка информационных

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	вычислительных ресурсов между пользователями, а также мер межсетевого экранирования дискредитируемой информационной системы и контроля подлинности сетевых запросов на сторонних серверах.	сообщений с использованием вычислительных мощностей оператора и (или) от его имени.
УБИ.156	Угроза утраты носителей информации	Внутренний нарушитель с низким потенциалом H1, H2	Носитель информации	Использование слабостей мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных.	Разглашение персональных данных граждан. Разглашение персональных данных граждан. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
					обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель с низким потенциалом H1	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	Использование слабостей мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Физический доступ к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Причинение имущественного ущерба.
УБИ.158	Угроза форматирования носителей информации	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с	Носитель информации	Использование слабости мер ограничения доступа к системной функции форматирования носителей информации.	Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Необходимость

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		низким потенциалом H1			изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций).
УБИ.159	Угроза «форсированного веб-браузинга»	Внешний нарушитель с низким потенциалом H1	Сетевой узел, сетевое программное обеспечение	Использование слабостей (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах.	Нарушение конфиденциальности (утечка) персональных данных.
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель с низким потенциалом H1	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	Использование слабостей мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Физический доступ к АРМ, носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	Нарушение конфиденциальности (утечка) персональных данных. Причинение имущественного ущерба.
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Внутренний нарушитель с низким	Системное программное обеспечение,	Внедрение вредоносного программного обеспечения.	Нарушение конфиденциальности (утечка) персональных

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	прикладное программное обеспечение	Использование слабостей в механизме подписывания программного кода.	данных. Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Внутренний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	Внедрение вредоносного программного обеспечения Использование слабостей механизмов фильтрации сетевого	Нарушение конфиденциальности (утечка) персональных данных.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		Н1, Н2		трафика и антивирусного контроля на уровне организации.	Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Внешний нарушитель с низким потенциалом Н1	Сетевое программное обеспечение	Использование недостаточностью мер контроля за активностью/существованием ящиков электронной почты.	Утечка конфиденциальной информации. Невозможность

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
					решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.170	Угроза неправомерного шифрования информации	Внешний нарушитель с низким потенциалом H1	Объект файловой системы	Внедрение вредоносного программного обеспечения	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Внешний нарушитель с низким потенциалом H1	Сетевой узел, сетевое программное обеспечение	Использование уязвимостей в сетевом программном обеспечении и слабостей механизмов антивирусного контроля и межсетевого экранирования. Внедрение вредоносного программного обеспечения.	Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением.
УБИ.172	Угроза распространения «почтовых червей»	Внешний нарушитель с низким потенциалом H1	Сетевое программное обеспечение	Внедрение вредоносного программного обеспечения.	Утечка конфиденциальной информации. Необходимость

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
					дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением.
УБИ.173	Угроза «спама» веб-сервера	Внешний нарушитель с низким потенциалом H1	Сетевое программное обеспечение	Использование уязвимостей механизмов фильтрации сообщений, поступающих из сети Интернет.	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.174	Угроза «фарминга»	Внешний нарушитель с низким потенциалом H1	Рабочая станция, сетевое программное обеспечение, сетевой трафик	Использование уязвимостей DNS-сервера, маршрутизатора	Нарушение конфиденциальности (утечка) персональных данных.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
УБИ.175	Угроза «фишинга»	Внешний нарушитель с низким потенциалом H1	Рабочая станция, сетевое программное обеспечение, сетевой трафик	Использование недостаточности знаний пользователей о методах и средствах «фишинга».	Нарушение конфиденциальности Нарушение конфиденциальности (утечка) персональных данных.
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Внутренний нарушитель с низким потенциалом H1, H2	Системное программное обеспечение, сетевое программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	Использование некорректно реализованных (или отсутствующие) средств реагирования на неправильные, самопроизвольные действия оператора, средств учёта нижних/верхних пределов скорости и направления реакции оператора, схемы реагирования на двойное нажатие клавиш при вводе обычных и критических данных, процедуры формирования временных пауз с возможностью выбора разных ответов (да/нет и т.п.).	Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	Использования имеющихся или предварительно внедрённых стандартных (известных и обычно не определяемых антивирусными программами как вредоносных) системных и сетевых утилит,	Нарушение конфиденциальности (утечка) персональных данных.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		H1, H2 Внешний нарушитель с низким потенциалом H1		предназначенных для использования администратором для диагностики и обслуживания системы (сети).	Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким	Объекты файловой системы	Деструктивное физическое воздействие на машинный носитель информации или деструктивное программное воздействие (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нём	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		потенциалом Н1			
УБИ.182	Угроза физического устаревания аппаратных компонентов	Внутренний нарушитель с низким потенциалом Н1, Н2	Аппаратное средство	Использовании пользователями технических средств в условиях, не удовлетворяющих требованиям заданных их производителем	Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внутренний нарушитель с низким потенциалом Н1, Н2 Внешний нарушитель с низким потенциалом Н1	Средство защиты информации	Использование слабостей мер разграничения доступа к конфигурационным файлам средства защиты информации	Разглашение персональных данных граждан. Нарушение законодательства Российской Федерации. Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Внутренний нарушитель с низким потенциалом H1, H2	Сетевое программное обеспечение	Внедрение вредоносного программного обеспечения	Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	Внедрение вредоносного программного обеспечения	Утечка конфиденциальной информации. Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		Н1			Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Внутренний нарушитель с низким потенциалом Н1, Н2 Внешний нарушитель с низким потенциалом Н1	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	Использование уязвимостей программного обеспечения Угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путём эксплуатации уязвимостей программного обеспечения.	Нарушение конфиденциальности (утечка) персональных данных. Нарушение законодательства Российской Федерации. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.
УБИ.205	Угроза нарушения работы компьютера и	Внешний	Аппаратное	Ошибочные действия при установке	Необходимость

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
	блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	нарушитель с низким потенциалом H1	устройство, программное обеспечение	и настройке средства защиты информации, реализующее функцию блокирования файлов	изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций).
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Внутренний нарушитель с низким потенциалом H1, H2 Внешний нарушитель с низким потенциалом H1	Средство вычислительной техники, мобильное устройство	Внедрение вредоносного программного обеспечения	Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени.
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Внутренний нарушитель с низким потенциалом	Аппаратное устройство	Использование уязвимостей, связанных с ошибкой контроля доступа к памяти, основанных на спекулятивном выполнении	Нарушение конфиденциальности (утечка) персональных данных.

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
		H1, H2 Внешний нарушитель с низким потенциалом H1		инструкций процессора.	Нарушение прав гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Внутренний нарушитель с низким потенциалом H1, H2	Системное программное обеспечение	Использование слабостей процедуры проверки пользовательских данных, используемых при формировании конфигурационного файла для программного обеспечения администрирования	Утечка конфиденциальной информации. Нарушение прав гражданина,

№ п/п	Наименование УБИ	Нарушитель	Объект воздействия	Способ воздействия	Негативные последствия
				информационных систем	закрепленных в Конституции Российской Федерации и федеральных законах.

6.2 Описание возможных сценариев реализации угроз безопасности информации

Актуальность возможных угроз безопасности информации ИСПДн определяется наличием сценариев их реализации.

Сценарии реализации угроз безопасности информации определены для соответствующих способов реализации угроз безопасности информации ИСПДн, определенных ранее, и применительно к объектам воздействия и видам воздействия на них.

Описание основных тактик (тактических задач) и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации, приведено в Приложении 11 к Методическому документу «Методика оценки безопасности информации» (Утвержден ФСТЭК России 5 февраля 2021 г.).

6.3 Выводы об актуальности угроз безопасности

Таким образом, в ходе оценки угроз безопасности информации определены возможные угрозы безопасности информации и оценена их актуальность для ИСПДн, указанных в п.1.1 настоящего документа – актуальные угрозы безопасности информации представлены в таблице.

Перечень актуальных угроз безопасности информации ИСПДн указанных в п.1.1. настоящего документа

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
УБИ.004	Угроза аппаратного сброса пароля BIOS	Сброс паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера») наличия у нарушителя физического доступа к системному блоку компьютера	Использование уязвимостей системных (материнских) плат – наличие механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Физический доступ к системному блоку АРМ.
УБИ.006	Угроза внедрения кода или данных	T1.3, T1.5+T2.3-5, T2.7, T2.9, T2.12-13+T3.1-6, T3.14-16+T4.3, T4.5-7+T5.1-2, T6.3, T6.7+T7.10-12, T7.15, T7.21+T8.1, T8.6-7, T9.1, T9.5-6, T9.14+T10.4-6	Внедрение вредоносного программного обеспечения. Использование уязвимостей кода системного ПО.
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации	T1.5, T1.9, T2.1, T2.4, T2.10+T6.1, T6.2+T8.1, T8.8+T10.2	Доступ к АРМ пользователя через консоль.
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	T2.5	Использование слабостей технологий контроля за обновлением программного обеспечения BIOS/UEFI.
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	T3.7+T6.7, T6.9+T7.12, T7.23, T7.26 +T10.1	Использование слабостей мер контроля целостности конфигурационных файлов или библиотек, используемых приложениями.
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	T2.5+ T7.3+T10.1, T2.6, T2.7, T10.8	Использование уязвимостей программного обеспечения BIOS/UEFI.

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	T1.5+T2.1, T2.3, T2.5+T3.1, T3.14+T4.5+ +T5.2+T6.3+T7.1+T8.5+T10.10	Использование уязвимостей программ, распределяющих вычислительные ресурсы между задачами.
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	T1.3, T1.11+T2.4,5+T4.5+T6.3,8+ +T7.1, 12+T8.1,7+T10.1	Доступ через консоль АРМ, через локальную вычислительную сеть организации.
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	T1.5+T2.5+T3.4,5+T4.1+T5.1, T5.2+T6.3, T6.5, T6.8+T8.1+T9.1, T9.2, T9.13+T10.1, T10.7	Использование слабостей мер защиты cookies-файлов.
УБИ.018	Угроза загрузки нештатной операционной системы	T2.5+T7.3+T10.1, T10.8	Физический доступ к АРМ. Использование слабостей технологий разграничения доступа к управлению BIOS/UEFI.
УБИ.019	Угроза заражения DNS-кеша	T.1.7+T4.1+T2.3, T2.13+T3.9+ +T4.5+T5.8+T6.8+T7.11, T7.20+T8.5+T9.9+T10.2, T10.7	Использование слабостей механизмов проверки подлинности субъектов сетевого взаимодействия, а также уязвимостей DNS-сервера.
УБИ.022	Угроза избыточного выделения оперативной памяти	T1.5, T1.11+T2.1, T2.5, T2.7+T3.1, T3.6+T5.3,4+T6.3,7+T8.1,5+T10.10 T1.3, T1.5+T2.3, T2.5, T2.7+T3.1, T3.3+T4.5+T5.1-3+T6.3, T6.6, T6.8+T7.2, T7.4+ T8.1, T8.5+T9.5, T9.13+T10.10, 11	Внедрение вредоносного программного обеспечения.
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы	T1.2, T1.3, T1.5, T1.16+T2.6, T2.7+T3.2+T4.3-4+T5.9+T6.1+T7.4, T7.21+T8.4+T9.5-6+ T10.1-3, T10.7-11	Физический доступ к АРМ, серверу, ТКО, машинным носителям информации, содержащим защищаемую информацию, линиям связи между сервером основного центра обработки данных и АРМ.

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	T1.3, T1.5+T2.3, T2.5, T2.7+T3.3, T3.6, T3.7+T4.5, T4.6+T5.1-3 + T6.7 + T7.1 + T8.7 + T9.8 + T10.7	Внедрение вредоносного программного обеспечения, установка аппаратных закладок Установка аппаратных закладок.
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	T1.3, T1.11+T2.4,5+T3.16+T4.5+ T5.2+T6.7+T7.1, 12+T8.1+T10.1	Использование уязвимостей мер разграничения доступа к защищаемой информации, слабости фильтрации входных данных.
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	T1.6-8, T2.1, T2.2, T2.4, T2.10, T2.11+ T10.2	Использование уязвимостей устройств идентификации и аутентификации.
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	T1.5, T1.6, T1.9 + T4.1, T4.2 + T6.2, T6.4, T6.6 + T10.2	Использование слабостей мер разграничения доступа к программам и файлам.
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	T1.4+T2.13+T5.1+T6.7+ +T8.5+T9.1, T9.3, T9.5+	Использование слабостей протоколов (заложенных в них алгоритмов), ошибок, допущенных в ходе реализации протоколов, или уязвимостей, внедряемых автоматизированных средств проектирования/разработки.
УБИ.041	Угроза межсайтового скриптинга	T1.4, T1.7+T2.1, T2.5+T3.3, T3.9+T4.2+T5.2+T8.3+T9.2+T10.2	Внедрение вредоносного программного обеспечения.
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	T2.9, T2.10 + T10.1-6	Использование слабостей технологий разграничения доступа к BIOS/UEFI, его функций администрирования и обновления, со стороны операционной системы или каналов связи.
УБИ.049	Угроза нарушения целостности данных кеша	T1.8+T2.1, T2.5, T2.7+T3.2, T3.7, T3.8, T3.9+T6.8+T7.10+ T10.1 – T10.11	Использование слабостей в механизме контроля целостности данных в кеше.
УБИ.051	Угроза невозможности	T4.6	Использование ошибок в реализации программно-аппаратных компонентов

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
	восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания		компьютера, связанных с обеспечением питания.
УБИ.053	Угроза невозможности управления правами пользователей BIOS	T2.5+T7.3+T10.1, T10.8	Физический доступ к терминалу и, при необходимости, к системному блоку компьютера.
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	T1.8, T.11+T2.5, T2.8+T3.3+T4.1,2+T6.2+T7.2, T7.13+T8.1, T8.7+T9.13, T9.14+T10.1,2+T10.9	Использование слабостями механизма контроля доступа к настройкам браузера.
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	T1.4, T1.13, T1.14+T2.3,4+T5.2+ +T6.6, T6.8+T7.1+T8.1+T9.13,14+T10.1,7	Использование уязвимостей средств контроля доступа, ошибок в параметрах конфигурации данных средств или отсутствия указанных средств.
УБИ.069	Угроза неправомерных действий в каналах связи	T1.4+T2.13+T5.3,11+T7.6+T8.5+ +T9.3+T10.1,5	Использование слабостей сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных.
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	T10.1, T10.7-8	Использование слабостей механизма удаления информации с машинных носителей.
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	T2.5+T3.10, T3.11+T7.3+T10.1, T10.8	Использование слабостей мер по разграничению доступа к управлению механизмом защиты BIOS/UEFI от записи, а также уязвимостей механизма обновления BIOS/UEFI, приводящих к переполнению буфера.
УБИ.074	Угроза несанкционированного доступа к аутентификационной	T1.9+T6.1, T6.5+ T10.2	Доступ через локальную вычислительную сеть организации Физический доступ к машинным носителям информации.

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
	информации		
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	T1.4-5+T2.3+T3.15+T4.2+T5.1+ +T6.9+T7.2+T8.5+T9.1+T10.1	Использование слабостей мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных).
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	T1.5, T2.10, T2.11, T4.1+T6.8+T7.1+T7.13+ T10.2	Использование слабостей мер разграничения доступа к информации аутентификации.
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	T2.5+T3.10, T3.11+T7.3+T10.1, T10.8	Использование потенциально опасных возможностей BIOS/UEFI.
УБИ.088	Угроза несанкционированного копирования защищаемой информации	T1.3-5+T2.3, T2.5, T2.7+T3.1,3+T4.2,7+ +T6.8+T7.4+T8.1,4,6+T9.10, T9.13,14+T10.1	Использование слабостей механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне.
УБИ.089	Угроза несанкционированного редактирования реестра	T1.3,5, T1.11+T2.3, T2.5, T2.8+T3.14, T3.16+T4.5+T5.2, T5.6+T6.6,7+T7.2,16+T8.1,2 +T9.2,5,6+T10.1,10	Использование слабостей механизма контроля доступа, заключающимися в присвоении реализующим его программам слишком высоких привилегий при работе с реестром.
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	T1.5,9+T2.5,8+T3.1,15+T4.1+ T6.1, T6.2, T6.3, T6.4+T7.2,13+T9.2, 13,14+T10.1,2	Использование слабостей механизмов разграничения доступа к защищаемой информации.
УБИ.091	Угроза несанкционированного удаления защищаемой	T2.5,7,8+T3.1+T4.1-3+ +T5.1,2+T6.2,3+T7.3+T8.1+T10.8	Использование уязвимостей в программном обеспечении, реализующих меры по обеспечению доступности защищаемой информации в системе.

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
	информации		
УБИ.093	Угроза несанкционированного управления буфером	Т3.7, Т3.9 + Т5.3, Т5.6 + Т9.2	Использование слабостей в механизме разграничения доступа к буферу обмена, а также слабостей в механизмах проверки вводимых данных.
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Т1.4, Т1.16+Т2.3+Т3.4+Т4.3+ +Т6.8+Т7.4+Т9.4+Т10.7	Использование уязвимостей и ошибок конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе.
УБИ.099	Угроза обнаружения хостов	Т1.4, Т1.16+Т2.3+Т3.4+Т4.3+ +Т6.8+Т7.4+Т9.4+Т10.7	Использование слабостей механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой систем.
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Т2.4, Т2.11+Т4.1+Т6.7, Т6.8+Т9.13+Т10.2, Т10.7	Использование некорректных значений параметров конфигурации средств аутентификации и/или отсутствием контроля входных данных.
УБИ.103	Угроза определения типов объектов защиты	Т1.5, Т1.11	Использование ошибок в параметрах конфигурации средств межсетевого экранирования, а также отсутствия механизмов контроля входных и выходных данных.
УБИ.104	Угроза определения топологии вычислительной сети	Т1.4, Т1.16+Т2.3+Т3.4+Т4.3+ +Т6.8+Т7.4+Т9.4+Т10.2	Использование слабостей механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями средств межсетевого экранирования (алгоритма работы и конфигурации правил фильтрации сетевого трафика).
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Т5.5	Использование свойств оперативной памяти обнулять своё состояние при выключении и перезагрузке. Физический доступ к АРМ.

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	T1.5+T2.5, T2.7+T3.4, T3.8+T4.5+T5.13+ +T6.7+T7.1, T7.10, T7.19+T8.1, T8.6+T9.8+T10.2, T10.3	Установка и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др.
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	T1.4+T2.13+T5.3,11+T7.6+T8.5+ +T9.3+T10.1,5	Использование слабостей механизмов сетевого взаимодействия, предоставляющими сторонним пользователям открытые данные о дискредитируемой системе, а также ошибки конфигурации сетевого программного обеспечения.
УБИ.121	Угроза повреждения системного реестра	T1.3,5, T1.11+T2.3, T2.5, T2.8+T3.14, T3.16+T4.5+T5.2, T5.6+T6.6,7+T7.2,16+T8.1,2 +T9.2,5,6+T10.1,10	Использование слабостей мер контроля доступа к файлам, содержащим данные реестра, мер резервирования и контроля целостности таких файлов, а также мер восстановления работоспособности реестра из-за сбоев в работе операционной системы.
УБИ.123	Угроза подбора пароля BIOS	T4.1+T6.2+ T10.1, T10.8	Физический доступ к АРМ. Использование слабостей механизма аутентификации, реализуемого в консолях BIOS/UEFI.
УБИ.124	Угроза подделки записей журнала регистрации событий	T1.4+T2.5+T3.1,6+T4.5+T6.3+T7.2, T7.3, T7.4, T7.6+T10.2, T10.5	Использование недостаточности мер по разграничению доступа к журналу регистрации событий безопасности.
УБИ.128	Угроза подмены доверенного пользователя	T1.5, T1.14+T2.3, T2.10, T2.13+T3.6+T4.1+T10.5,7	Использование слабостей технологий сетевого взаимодействия, зачастую не позволяющие выполнить проверку подлинности источника/получателя информации.
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	T 2.6+T 3.2+T 4.6+T 6.2+ T 7.22+ T10.1, T 10.6	Физический доступ к АРМ. Использование недостаточности мер разграничения доступа и контроля целостности резервных копий программного обеспечения BIOS/UEFI.

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
УБИ.130	Угроза подмены содержимого сетевых ресурсов	T1.4, T1.5, T1.10+T2.13+T3.7+T4.2+ +T6.8+T7.23-25+T8.7+T9.13+ T10.1, T10.3, T10.4, T10.7	Использование слабостей технологий сетевого взаимодействия, зачастую не позволяющие выполнить проверку подлинности содержимого электронного сообщения.
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	T1.4+T2.1+T5.3, T5.8+T6.7+T7.4,8+ + T10.10	Использование слабостей сетевых технологий, связанных с ограниченностью скорости обработки потоков сетевых запросов, и недостаточностью мер контроля за управлением соединениями и ошибками реализации сетевых протоколов.
УБИ.144	Угроза программного сброса пароля BIOS	T4.1+T6.2+ T10.1, T10.8	Физический доступ к АРМ для несанкционированного доступа к настройкам BIOS/UEFI после перезагрузки компьютера путём ввода «пустого» пароля. Использование слабостей мер разграничения доступа в операционной системе к функции сброса пароля BIOS/UEFI.
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	T1.1+T2.8+T3.1+T4.5+T5.6+ +T6.3, T6.9+T8.1+T9.5+T10.2, T10.3	Внедрение вредоносного программного обеспечения.
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	T4.1+T2.1, T2.5+T3.14+T8.1+T10.2	Использование недостаточности мер по обеспечению конфиденциальности информации, реализованных в WSDL-сервисах, предоставляющих подробные сведения о портах, службах и соединениях, доступных пользователям.
УБИ.152	Угроза удаления	T1.5, T2.10, T2.11, T4.1+T6.8+T7.1+T7.13+	Использование слабостей политики разграничения доступа к аутентификационной информации и средствам работы с учётными записями

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
	аутентификационной информации	Т10.2	пользователей.
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Т1.4+Т2.1+Т5.3, Т5.8+Т6.7+Т7.4,8+ + Т10.10	Использование слабостей мер межсетевого экранирования дискредитируемой информационной системы, мер контроля подлинности сетевых запросов на сторонних серверах, а также слабостей модели взаимодействия открытых систем.
УБИ.155	Угроза утраты вычислительных ресурсов	Т1.5+Т2.1, Т2.3, Т2.5+Т3.1, Т3.14+Т4.5+ +Т5.2+Т6.3+Т7.1+Т8.5+Т10.10	Использование слабостей механизма контроля за распределением вычислительных ресурсов между пользователями, а также мер межсетевого экранирования дискредитируемой информационной системы и контроля подлинности сетевых запросов на сторонних серверах.
УБИ.156	Угроза утраты носителей информации	Утеря машинного носителя информации (например, съемного носителя информации) с защищаемой информацией или потеря информации из-за отсутствия резервного копирования.	Использование слабостей мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных.
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Т 6.8	Использование слабостей мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Физический доступ к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.).
УБИ.158	Угроза форматирования носителей информации	Т1.3-5+Т2.3,5+Т3.1+Т4.1+ +Т6.3+Т 7.3+Т 10.8	Использование слабости мер ограничения доступа к системной функции форматирования носителей информации.
УБИ.159	Угроза «форсированного веб-браузинга»	Т1.3, Т1.6+Т2.1, Т2.5+Т5.2+Т6.3+ +Т7.1+Т8.2+Т10.1, Т10.3	Использование слабостей (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах.

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Т 6.8	Использование слабостей мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Физический доступ к АРМ, носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Т 6.3 + Т 10.2, Т 10.3	Внедрение вредоносного программного обеспечения. Использование слабостей в механизме подписывания программного кода.
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Т1.1+Т2.8+Т3.3+Т4.5+Т5.2+ +Т6.4+Т7.1+Т8.4+Т9.13+Т10.2, Т10.3	Внедрение вредоносного программного обеспечения Использование слабостей механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации.
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Т 1.3, Т 1.5, Т 1.8, Т 1.11	Использование недостаточностью мер контроля за активностью/существованием ящиков электронной почты.
УБИ.170	Угроза неправомерного шифрования информации	Т1.1+Т2.8+Т3.1, Т3.3+Т4.5+Т5.2+ +Т6.7+Т7.1+Т8.7+Т9.8+ Т10.1	Внедрение вредоносного программного обеспечения.
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Т1.1+Т2.3, Т2.8+ Т3.1, Т3.3+Т4.3+ +Т5.4+Т6.7+Т7.2, Т7.12, Т7.21+Т8.5+Т9.6+Т10.2, Т10.11	Использование уязвимостей в сетевом программном обеспечении и слабостей механизмов антивирусного контроля и межсетевого экранирования. Внедрение вредоносного программного обеспечения.
УБИ.172	Угроза распространения «почтовых червей»	Т1.1, Т1.14+Т2.1, Т2.8+Т3.1+Т4.5+ +Т5.3+Т6.7+Т7.10, Т7.15+Т8.3+Т9.3+Т10.3	Внедрение вредоносного программного обеспечения.

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
УБИ.173	Угроза «спама» веб-сервера	Т 1.5, Т 1.8+ Т 2.1+ Т 5.12+ Т 9.11	Использование уязвимостей механизмов фильтрации сообщений, поступающих из сети Интернет.
УБИ.174	Угроза «фарминга»	Т1.3, Т1.5, Т1.7+Т2.1, Т2.3+Т3.3+Т4.2+Т5.3+Т6.3,4+ +Т7.20+Т8.1+Т9.2+Т10.2,3	Использование уязвимостей DNS-сервера, маршрутизатора.
УБИ.175	Угроза «фишинга»	Т1.1, Т1.11+Т2.8+Т3.1, Т3.3+Т4.5+Т5.2,3+ +Т6.4,7+Т7.1+Т8.1,4+Т9.5, 13+ Т10.2, Т10.3	Использование недостаточности знаний пользователей о методах и средствах «фишинга».
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Т 2.4+Т 10.2, Т 10.3	Использование некорректно реализованных (или отсутствующие) средств реагирования на неправильные, самопроизвольные действия оператора, средств учёта нижних/верхних пределов скорости и направления реакции оператора, схемы реагирования на двойное нажатие клавиш при вводе обычных и критических данных, процедуры формирования временных пауз с возможностью выбора разных ответов (да/нет и т.п.).
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Т1.3-5+Т2.5,8+Т3.6+Т4.1,2+ +Т5.1,2+Т6.3+Т7.1+Т8.1,3+Т1.1,2,10	Использования имеющихся или предварительно внедрённых стандартных (известных и обычно не определяемых антивирусными программами как вредоносных) системных и сетевых утилит, предназначенных для использования администратором для диагностики и обслуживания системы (сети).
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Т 1.4+Т 10.2	Деструктивное физическое воздействие на машинный носитель информации или деструктивное программное воздействие (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нём.
УБИ.182	Угроза физического устаревания аппаратных компонентов	Т 2.6	Использовании пользователями технических средств в условиях, не удовлетворяющих требованиям заданных их производителем.

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Т2.3, Т2.4+Т6.7-8+Т7.2, Т7.4, Т7.6 + Т10.2, Т10.10	Использование слабостей мер разграничения доступа к конфигурационным файлам средства защиты информации.
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Т1.1, Т1.11+Т2.8+Т3.3+Т4.5+Т5.2+ +Т6.4+Т7.1+Т8.4+Т9.13+ Т10.2, Т10.3	Внедрение вредоносного программного обеспечения.
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Т1.1, Т1.16+Т2.12+Т3.8-11+Т4.5-6+Т5.1+Т6.6-7+Т7.9, Т7.24-27+Т8.7+Т9.13	Внедрение вредоносного программного обеспечения.
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Т1.5, Т1.8+Т2.3, Т2.5+Т3.5 +Т4.6+Т5.6+ Т6.3-4, Т6.7-9+Т7.21-22+Т8.1+ Т9.4+Т10.1-11	Использование уязвимостей программного обеспечения. Угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путём эксплуатации уязвимостей программного обеспечения.
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Т 2.3+ Т 6.7+ Т 7.6	Ошибочные действия при установке и настройке средства защиты информации, реализующее функцию блокирования файлов.
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Т1.1+Т2.3, Т2.8+ Т3.1, Т3.3+Т4.3+Т5.4+Т6.7+Т7.2, Т7.12, Т7.21+ Т8.5 + Т9.6+ Т10.2, Т10.11	Внедрение вредоносного программного обеспечения.
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Т 2.6 + Т 6.7	Использование уязвимостей, связанных с ошибкой контроля доступа к памяти, основанных на спекулятивном выполнении инструкций процессора.

№ п/п	Наименование УБИ	Сценарий реализации УБИ	Способ воздействия
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Т 10.2, Т 10.5	Использование слабостей процедуры проверки пользовательских данных, используемых при формировании конфигурационного файла для программного обеспечения администрирования информационных систем Защищаемая информация, в т.ч. ПДн для ИСПДн, указанных в п.1.1.11

7. Использование средств криптографической защиты информации для обеспечения безопасности персональных данных

Использование средств криптографической защиты информации для обеспечения безопасности персональных данных указано в Приложении №1.

Разработчик:
Специалист по защите информации отдела
информатизации образовательного
и производственного процессов С.А.Бабин

СОГЛАСОВАНО

Зам. директора по ПО
_____ Е.В.Бурдин
_____ 2023
Начальник отдела ИО и ПП
_____ С.В.Ваганов
06.10. 2023
Начальник отдела ДОУ
_____ А.В.Шорина
06.10. 2023

Приложение №1

к «Частной модели угроз безопасности персональных данных в информационных системах персональных данных Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Политехнический колледж городского хозяйства»

Использование средств криптографической защиты информации для обеспечения безопасности персональных данных

Приложение разработано в соответствии с Приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 г. Москва «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», методический документ ФСБ, а также Приказ ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну». Описание информационной системы и нарушителей изложены в разделе 4 настоящей Модели угроз.

1. Использование СКЗИ

Исходя из анализа режима обработки информации, определено, что передача персональных данных осуществляется по каналам связи, выходящими за пределы контролируемой зоны и не защищенным от перехвата нарушителем передаваемой по ним информации (передача персональных данных по информационно-телекоммуникационным сетям общего пользования) и возможно несанкционированное воздействие на эту информацию. В связи с этим для обеспечения безопасности персональных данных необходимо использование средств криптографической защиты информации (далее – СКЗИ), прошедшие в установленном порядке процедуру оценки соответствия.

При этом необходимо учитывать следующее:

– криптографическая защита персональных данных может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ;

– СКЗИ штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СКЗИ требований и которые образуют среду функционирования СКЗИ;

– СКЗИ не предназначены для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СКЗИ не предназначены для защиты персональных данных от раскрытия лицами, которым предоставлено право на доступ к этой информации);

– СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований, действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ;

– для обеспечения безопасности персональных данных при их обработке в ИСПДн должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия. Перечень СКЗИ, сертифицированных ФСБ России, опубликован на официальном сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России (www.clsz.fsb.ru). Дополнительную информацию о конкретных средствах защиты информации необходимо получать из эксплуатационной документации, а также непосредственно у разработчиков или производителей этих средств и, при необходимости, у специализированных организаций, проводивших тематические исследования этих средств;

– СКЗИ являются как средством защиты персональных данных, так и объектом защиты.

2. Описание каналов атак

Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в ИСПДн, являются:

– каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);

– штатные программно-технические средства ИСПДн;

– коммутационное оборудование, расположенное в пределах контролируемой зоны, не защищенное от НСД к информации организационно-техническими мерами;

– электронные носители, в том числе съемные, сданные в ремонт и вышедшие из употребления; неучтенные носители информации;

– кабельные системы, расположенные, как в пределах контролируемой зоны, так и за ее пределами, не защищенные от НСД к информации организационно-техническими мерами.

–

3. Обобщенные возможности источников атак

На основании анализа исходных данных об ИСПДн, объектах защиты и источниках атак определены обобщенные возможности источников атак. Обобщенные возможности источников атак представлены в таблице ПА.3.1.

Таблица ПА.3.1 - Обобщенные возможности источников атак

№ п/п	Обобщенные возможности источников атак	Да/нет
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	да
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования	нет
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	нет
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	нет
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения);	нет
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ).	нет

4. Обоснование неактуальности угроз

В таблице ПА.4.1 приводятся организационно-технические меры, направленные на противодействие возможностям источников атак.

Таблица ПА.4.1 – Возможности нарушителей и меры противодействия угрозам атак

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	не актуально	Проводятся работы по подбору персонала; - доступ в контролируемую зону, где располагаются элементы ИСПДн, в том числе СКЗИ, обеспечивается в соответствии с

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
			контрольно-пропускным режимом; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены элементы ИСПДн, в том числе СКЗИ, и сотрудники, не являющиеся пользователями ИСПДн, находятся в этих помещениях только в присутствии ответственных сотрудников Учреждения; - сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации; - пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации; - помещения, в которых располагаются элементы ИСПДн, в том числе СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; - утверждены правила доступа в помещения, где располагаются элементы ИСПДн, в том числе СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях; - утвержден перечень лиц, имеющих право доступа в помещения, где располагаются элементы ИСПДн, в том числе СКЗИ; - осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; - осуществляется регистрация и учет действий пользователей с защищаемой информацией, в т.ч. персональными данными; - осуществляется контроль целостности средств защиты; - на АРМ (серверах), на которых установлены

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
			СКЗИ: - используются сертифицированные средства защиты информации от несанкционированного доступа; - используются сертифицированные средства антивирусной защиты.
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее – элементы ИСПДн), на которых реализованы СКЗИ и СФ.	не актуально	Проводятся работы по подбору персонала; - доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; - документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения.
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых	не актуально	Проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается ресурсы ИСПДн, обеспечивается в соответствии с контрольно-пропускным режимом; - сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу сотрудников; - сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации.

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
	реализованы СКЗИ и СФ.		
1.4	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	Проводятся работы по подбору персоналов; - помещения, в которых располагаются элементы ИСПДн, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; - сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации; - осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; - осуществляется регистрация и учет действий пользователей. В ИСПДн используются: - сертифицированные средства защиты информации от несанкционированного доступа; - сертифицированные средства антивирусной защиты.
2.1	Физический доступ к элементам ИСПДн, на которых реализованы СКЗИ и СФ.	не актуально	Проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается элементы ИСПДн, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются элементы ИСПДн, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода.
2.2	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в	не актуально	Проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается элементы ИСПДн, на которых реализованы СКЗИ и СФ,

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
	которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.		обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии ответственных сотрудников Учреждения.
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; - высокая стоимость и сложность подготовки реализации возможности; - проводятся работы по подбору персонала; - доступ в контролируемую зону и помещения, где располагается элементы ИСПДн, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии ответственных сотрудников Учреждения; - осуществляется разграничение и контроль доступа пользователей к защищаемым

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
			ресурсам; - осуществляется регистрация и учет действий пользователей; - на АРМ, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; - используются сертифицированные средства антивирусной защиты.
3.2	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; - высокая стоимость и сложность подготовки реализации возможности.
3.3	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; - высокая стоимость и сложность подготовки реализации возможности.
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; - высокая стоимость и сложность подготовки реализации возможности;

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
			- проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; - помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; - представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии ответственных сотрудников Учреждения; - осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; - осуществляется регистрация и учет действий пользователей; - на АРМ (серверах), на которых установлены СКЗИ: - используются сертифицированные средства защиты информации от несанкционированного доступа; - используются сертифицированные средства антивирусной защиты.
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.
4.3	Возможность воздействовать на любые компоненты СКЗИ и СФ.	не актуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности угроз
			интерес для реализации возможности.

5. Основные организационно-технические меры, необходимые для противодействия возможностям источников атак

Реализация угроз безопасности информации, обрабатываемых в информационной системе определяется возможностями источников атак. Для противодействия возможностями источников атак в Учреждении должны быть приняты следующие организационно-технические меры:

– на должности, в обязанности которых входят работа со средствами защиты, защищаемой информацией в том числе ПДн, назначаются ответственные добросовестные лица, имеющие положительные характеристики, ознакомленные с ответственностью за несоблюдение правил обеспечения безопасности информации, имеющие знания и навыки в работе со средствами вычислительной техники и защиты информации;

– организован контрольно-пропускной режим в помещения с элементами ИСПДн и/или СКЗИ;

– определен порядок доступа в помещения с элементами ИСПДн и/или СКЗИ, лиц, не имеющих допуска к защищаемой информации;

– помещения, в которых располагаются элементы ИСПДн и/или СКЗИ, должны быть оснащены входными дверьми с замками;

– обеспечение постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода;

– утверждены правила доступа в помещения, где располагаются элементы ИСПДн и СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях;

– назначены лица, отвечающие за администрирование информационной системы, безопасность информации и эксплуатацию СКЗИ;

– утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ;

– документация на СКЗИ хранится у ответственного за СКЗИ в металлическом ящике;

– осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;

– осуществляется регистрация и учет действий пользователей с защищаемой информацией;

– осуществляется контроль целостности средств защиты;

– на элементах ИСПДн (АРМ), на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа и антивирусной защиты;

– ограничена возможность изменения настроек BIOS (установлен пароль), запрещена загрузка операционной системы с внешних носителей информации.

6. Определение класса, применяемого СКЗИ

Исходя из анализа данных, представленных в Приложении 1 и при выполнении мер, изложенных в пункте ПА.6, в соответствии с требованиями Приказа ФСБ России от 10.07.2014 № 378 для нейтрализации атак достаточно применение СКЗИ класса КС1 и выше (если иное не оговорено в эксплуатационной документации на систему).

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

к «Частной модели угроз безопасности персональных данных в информационных системах персональных данных Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Политехнический колледж городского хозяйства»

Информация о внесенных изменениях					
№ изменения	№ листа	№ и дата приказа	Дата внесения изменения	Дата введения изменения в действие	Подпись лица, внесшего изменения
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					

Информация о проведении актуализации		
Дата ежегодной актуализации	Результаты актуализации	Подпись разработчика