АКАДЕМИЯ АЙТИ
a Softline Company

academyit.ru

Меры и средства защиты конфиденциальной информации от несанкционированного доступа

АКАДЕМИЯ АЙТИ
a Softline Company

academyit.ru

Разработка модели угроз безопасности информации (практическое задание)

Модель угроз безопасности информации

Модель угроз (безопасности информации): физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

ГОСТ Р 50922-2006

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Для определения **угроз безопасности информации** и разработки **модели угроз безопасности информации** применяются методические документы, разработанные и утвержденные ФСТЭК России.

Приказ ФСТЭК России от 11 февраля 2013 г. N 17

Порядок оценки угроз безопасности информации

Оценка угроз безопасности информации проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях с заданной архитектурой и в условиях их функционирования – актуальных угроз безопасности информации.

Основные задачи, решаемые в ходе оценки угроз безопасности информации:

- определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
- инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;
- определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
- оценка способов реализации (возникновения) угроз безопасности информации;
- оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;
- оценка сценариев реализации угроз безопасности информации в системах и сетях.

МД ФСТЭК России. Методика оценки угроз безопасности информации, 05.02.2021

Порядок оценки угроз безопасности информации

а) исходные данные для оценки угроз безопасности информации: общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с Положением о ФСТЭК, утвержденного Указом Президента РФ от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) описания векторов (шаблоны) компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) документация на системы и сети (а именно: техническое задание на создание систем и сетей, частное техническое задание на создание системы защиты, программная (конструкторская) и эксплуатационная (руководства, инструкции) документация, содержащая сведения о назначении и функциях, составе и архитектуре систем и сетей, о группах пользователей и уровне их полномочий и типах доступа, о внешних и внутренних интерфейсах, а также иные документы на системы и сети, разработка которых предусмотрена требованиями по защите информации (обеспечению безопасности) или национальными стандартами);

МД ФСТЭК России. Методика оценки угроз безопасности информации, 05.02.2021

Порядок оценки угроз безопасности информации

г) договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в случае функционирования систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры);

д) нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и функционируют системы и сети, содержащие в том числе описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;

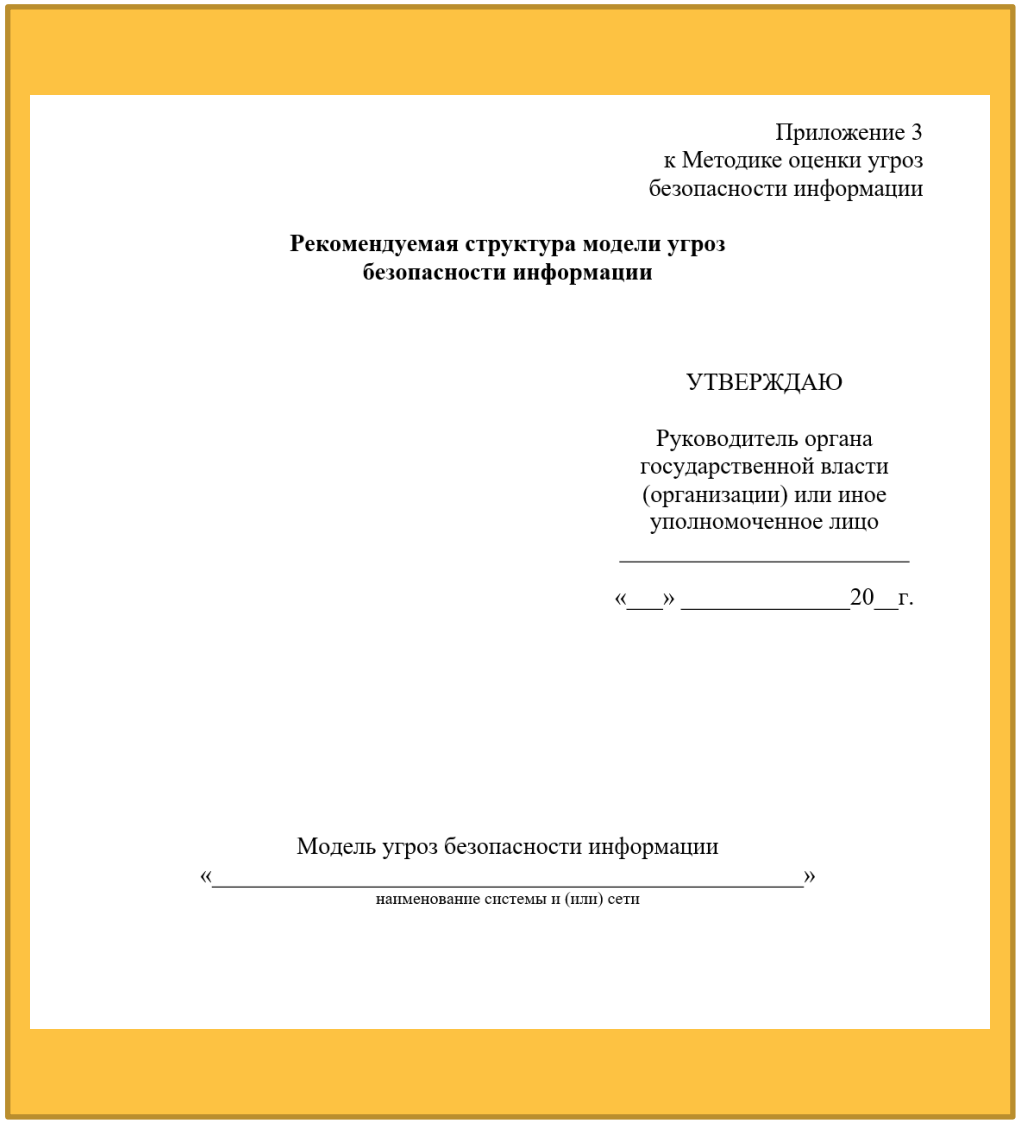
е) технологические, производственные карты или иные документы, содержащие описание управленческих, организационных, производственных и иных основных процессов (бизнес-процессов) в рамках выполнения функций (полномочий) или осуществления видов деятельности обладателя информации, оператора (далее – основные (критические) процессы);

ж) результаты оценки рисков (ущерба), проведенной обладателем информации и (или) оператором.

МД ФСТЭК России. Методика оценки угроз безопасности информации, 05.02.2021

Порядок оценки угроз безопасности информации

Результаты оценки угроз безопасности информации отражаются в модели угроз, которая представляет собой описание систем и сетей и актуальных угроз безопасности информации. Рекомендуемая структура модели угроз безопасности информации приведена в *приложении 3 к Методике оценки угроз безопасности информации, 05.02.*



Приложение 3
к Методике оценки угроз
безопасности информации

Рекомендуемая структура модели угроз безопасности информации

УТВЕРЖДАЮ

Руководитель органа
государственной власти
(организации) или иное
уполномоченное лицо

_____

«___» _____20__г.

Модель угроз безопасности информации

«_____»

наименование системы и (или) сети

МД ФСТЭК России. Методика оценки угроз безопасности информации, 05.02.2021

Рекомендуемая структура модели угроз безопасности информации

1. Общие положения

Раздел «Общие положения» содержит:

- назначение и область действия документа;
- нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз;
- наименование обладателя информации, заказчика, оператора систем и сетей;
- подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей;
- наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии).

МД ФСТЭК России. Методика оценки угроз безопасности информации, 05.02.2021

Рекомендуемая структура модели угроз безопасности информации

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

Раздел «Описание систем и сетей и их характеристика как объектов защиты» содержит:

- наименование систем и сетей, для которых разработана модель угроз безопасности информации;
- класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных;
- нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети;
- назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим;
- основные процессы (бизнес-процессы) обладателя информации, оператора, для обеспечения которых создаются (функционируют) системы и сети;
- состав и архитектуру систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей;

МД ФСТЭК России. Методика оценки угроз безопасности информации, 05.02.2021

Рекомендуемая структура модели угроз безопасности информации

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

Продолжение раздела «Описание систем и сетей и их характеристика как объектов защиты» содержит:

- описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включаются все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация (например, предоставлен доступ к сайту без прохождения авторизации);
- описание внешних интерфейсов и взаимодействий систем и сетей с пользователями (в том числе посредством машинных носителей информации, средств ввода-вывода, веб-приложений), иными системами и сетями, обеспечивающими системами, в том числе с сетью «Интернет»;
- информацию о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, о модели предоставления вычислительных услуг, о распределении ответственности за защиту информации между обладателем информации, оператором и поставщиком вычислительных услуг, об условиях использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (при наличии).

К модели угроз безопасности информации могут прилагаться схемы и рисунки, иллюстрирующие состав и архитектуру систем и сетей, интерфейсы взаимодействия компонентов системы и сети, группы пользователей, а также другие поясняющие материалы.

Рекомендуемая структура модели угроз безопасности информации

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

Раздел «Возможные негативные последствия от реализации (возникновения) угроз безопасности информации» содержит:

- описание видов рисков (ущербов), актуальных для обладателя информации, оператора, которые могут наступить от нарушения или прекращения основных процессов;
- описание негативных последствий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к возникновению рисков (ущерба).

МД ФСТЭК России. Методика оценки угроз безопасности информации, 05.02.2021

Рекомендуемая структура модели угроз безопасности информации

4. Возможные объекты воздействия угроз безопасности информации

Раздел «Возможные объекты воздействия угроз безопасности информации» содержит:

- наименования и назначение компонентов систем и сетей, которые непосредственно участвуют в обработке и хранении защищаемой информации, или обеспечивают реализацию основных процессов обладателя информации, оператора;
- описание видов воздействия на компоненты систем и сетей, реализация которых нарушителем может привести к негативным последствиям.
- К модели угроз безопасности информации может прилагаться схема с отображением объектов воздействия и их назначения в составе архитектуры систем и сетей.

МД ФСТЭК России. Методика оценки угроз безопасности информации, 05.02.2021

Рекомендуемая структура модели угроз безопасности информации

5. Источники угроз безопасности информации

Раздел «Источники угроз безопасности информации» содержит:

- характеристику нарушителей, которые могут являться источниками угроз безопасности информации, и возможные цели реализации ими угроз безопасности информации;
- категории актуальных нарушителей, которые могут являться источниками угроз безопасности информации;
- описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей.
- К модели угроз безопасности информации могут прилагаться рисунки, иллюстрирующие возможности нарушителей, и другие поясняющие материалы.

МД ФСТЭК России. Методика оценки угроз безопасности информации, 05.02.2021

Рекомендуемая структура модели угроз безопасности информации

6. Способы реализации (возникновения) угроз безопасности информации

Раздел «Способы реализации (возникновения) угроз безопасности информации» включает:

- описание способов реализации (возникновения) угроз безопасности информации, которые могут быть использованы нарушителями разных видов и категорий;
- описание интерфейсов объектов воздействия, доступных для использования нарушителями способов реализации угроз безопасности информации.

К модели угроз безопасности информации может прилагаться схема с отображением типов логических, физических интерфейсов объектов воздействия, в том числе требующих физического доступа к ним, а также соответствующие им способы реализации угроз безопасности информации.

МД ФСТЭК России. Методика оценки угроз безопасности информации, 05.02.2021

Рекомендуемая структура модели угроз безопасности информации

7. Актуальные угрозы безопасности информации

Раздел «Актуальные угрозы безопасности информации» включает:

- перечень возможных (вероятных) угроз безопасности информации для соответствующих способов их реализации и уровней возможностей нарушителей;
- описание возможных сценариев реализации угроз безопасности информации;
- выводы об актуальности угроз безопасности информации.

К модели угроз безопасности информации может прилагаться схема с отображением сценариев реализации угроз безопасности информации.

МД ФСТЭК России. Методика оценки угроз безопасности информации, 05.02.2021

Методика разработки модели угроз для информационной системы персональных данных (ИСПДн)

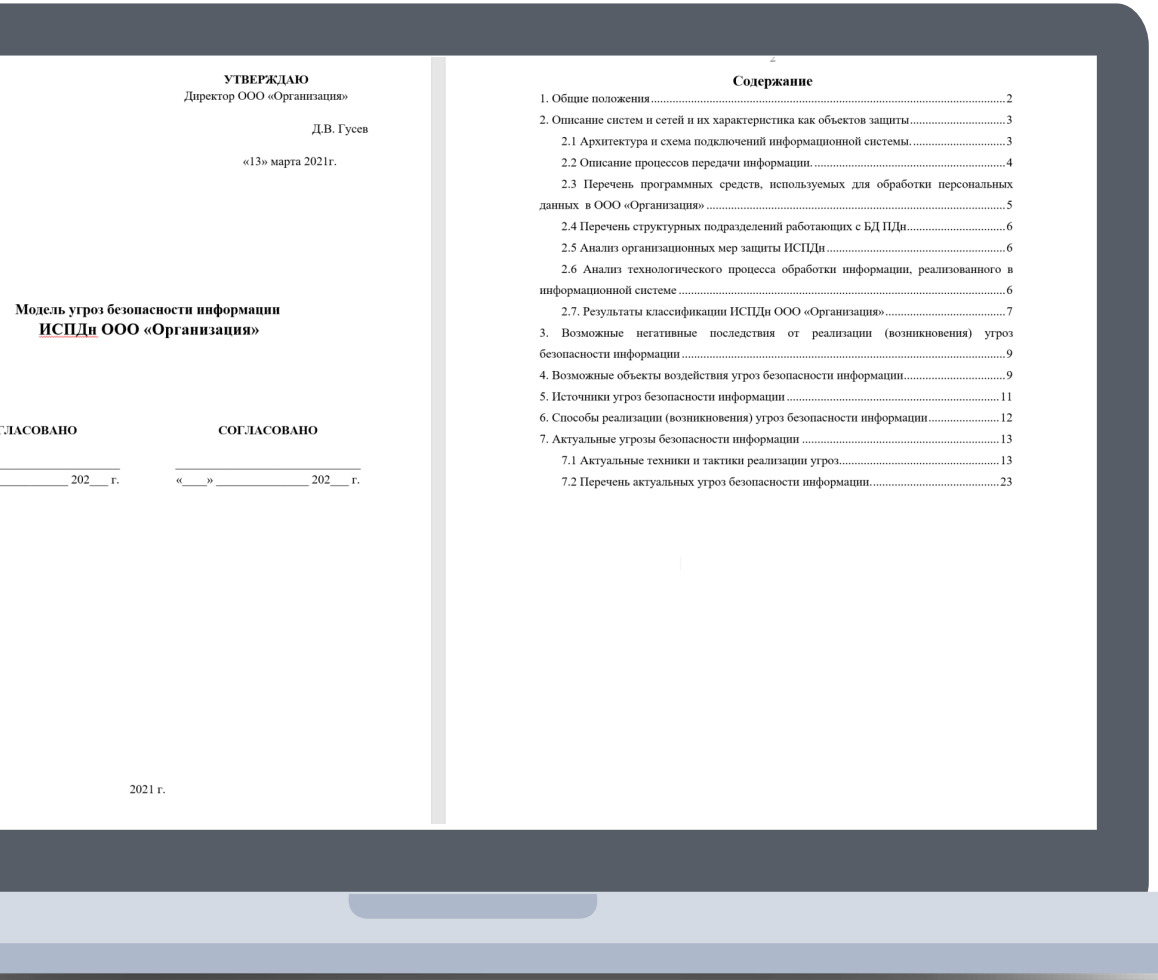
Определение угроз безопасности ПДн

- Базовая модель угроз безопасности ПДн при их обработке в ИСПДн, ФСТЭК, 2008.
- Методика оценки угроз безопасности информации, ФСТЭК, 2021.
- Банк данных угроз безопасности информации http://bdu.fstec.ru/threat
- .....

НМД ФСТЭК России

- Базовая модель угроз безопасности персональных данных при их обработке в ИСПДн, ФСТЭК, 2008.
- Методика оценки угроз безопасности информации, ФСТЭК, 2021
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн (приказ ФСТЭК от 18 февраля 2013 г. N 21
- МД ФСТЭК. Меры защиты информации в государственных информационных системах от 11.02.2014.

Определение угроз безопасности ПДн



УТВЕРЖДАЮ
Директор ООО «Организация»

Д.В. Гусев

«13» марта 2021г.

Модель угроз безопасности информации
ИСПДн ООО «Организация»

ГЛАСОВАНО

_____ 202___ г.

СОГЛАСОВАНО

_____

«____» _____ 202___ г.

2021 г.

Содержание

Разрабатываем Модель угроз безопасности персональных данных, обрабатываемых в информационной системе персональных данных (ИСПДн)

Последовательность разработки Модели угроз безопасности персональных данных, обрабатываемых в информационной системе персональных данных (ИСПДн)

1. Общие положения
2. Описание систем и сетей и их характеристика как объектов защиты
3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации
4. Возможные объекты воздействия угроз безопасности информации
5. Источники угроз безопасности информации
6. Способы реализации (возникновения) угроз безопасности информации
7. Актуальные угрозы безопасности информации

1. Общие положения

Модель угроз безопасности информации для ИСПДн ООО «Организация» разработана на основании следующих документов:

ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию;

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная Заместителем директора ФСТЭК России 15 февраля 2008 г;

«Методика оценки угроз безопасности информации», утвержденная Заместителем директора ФСТЭК России 5 февраля 2021 г.

Для разработки модели угроз безопасности информации на договорной основе была привлечена организация - ФГУП «НПП «Бэтта», аккредитованная ФСТЭК России в качестве органа по аттестации объектов информатизации (Аттестат аккредитации органа по аттестации №СЗИ RU.082/2.В29.274, Лицензия по ТЗКИ - регистрационный №0019 от 31 октября 2002г), совместно с начальником отдела по информационной безопасности (ИБ) ООО «Организация».

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

2.1 Архитектура и схема подключений информационной системы

Описание ИСПДн ООО «Организация» представлена в виде локальной вычислительной сети (ЛВС), объединенной в единую информационную систему средствами связи с использованием технологии удаленного доступа, имеющую выход в сеть международного информационного обмена (СМИО) «Интернет».....

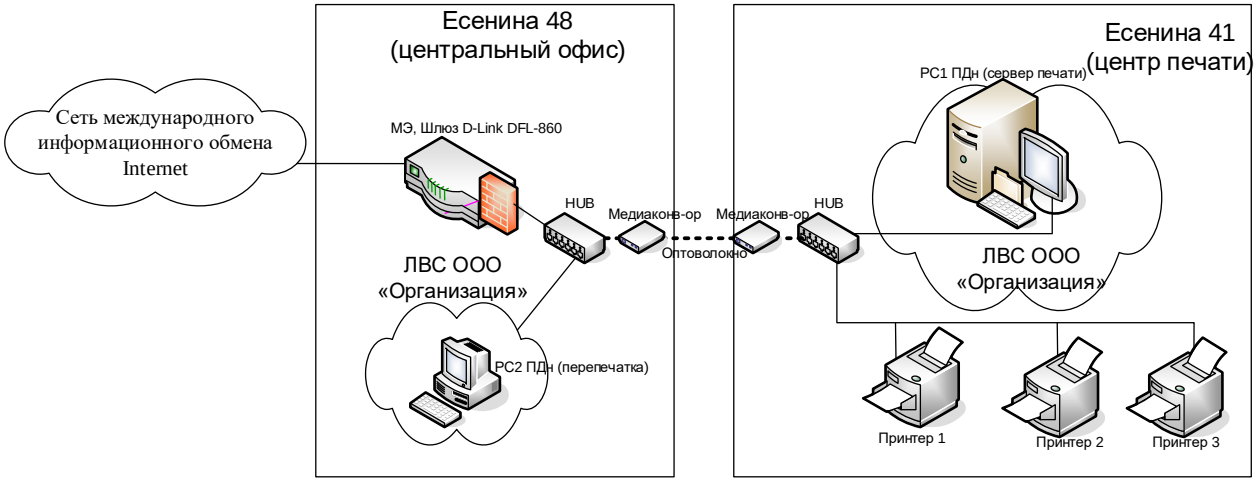


Рис. 1 - Схема ЛВС ООО «Организация»

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

2.2 Описание процессов передачи информации

В рабочем процессе ОАО «НСК» предоставляет персональные данные в ООО «Организация» в виде файлов формата DBF, данные передаются через открытые каналы СМИО «Интернет» по электронной почте в архиве WinRar. Обработка персональных данных в ИСПДн ООО «Организация» ведётся на рабочей станции №1 (сервер печати).....

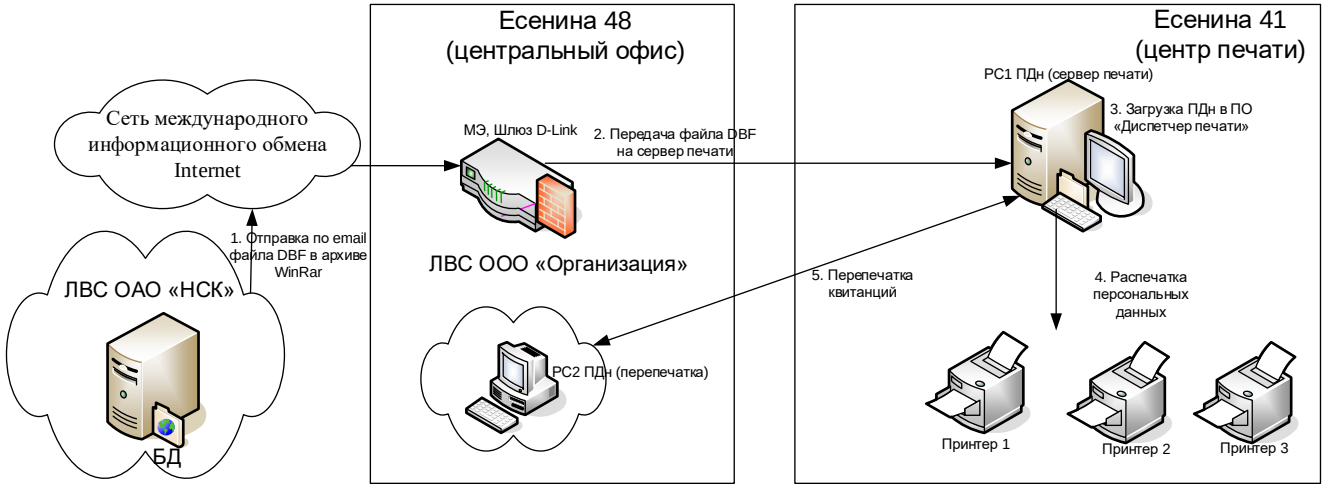


Рис. 2 - Схема потоков персональных данных в ИСПДн ООО «Организация».

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

2.3 Перечень программных средств, используемых для обработки персональных данных в ООО «Организация»

Обработка персональных данных в ИСПДн ООО «Организация» ведётся в специализированном программном обеспечении «Диспетчер печати».
Перечень имеющихся программных средств, используемых для обработки персональных данных приведены в таблице 1.

Таблица 1

№ п/п	Наименование ПС (ее составной части)	Расположение объекта	Технология обработки (АРМ, ЛВС, Распр)	Субъекты ПДн	Объем обрабатываемых Пдн (количество записей субъектов Пдн в базе данных ИС-	Описание режима работы с базой данных
1	2	3	4	9	10	11
1	«Диспетчер печати»	г. Москва, ул. Сергея Есенина, д. 41 – рабочая станция №1, ул. Сергея Есенина, д. 48 – рабочая станция №2	ЛВС, многопольз.	Не являются сотрудниками оператора	до 100 тыс	Локальная работа с базой на РС. Вход в систему по логину и паролю

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

2.4 Перечень структурных подразделений работающих с БД ПДн ООО «Организация»

Перечень структурных подразделений работающих с БД ПДн отображен в таблице 2.

Таблица 2

№ п/п	Наименование БД (ее составной части)	Расположение объекта	Структурное подразделение
1	2	3	4
1	База данных «Диспетчер печати»	г. Москва, ул. Сергея Есенина, д. 41 – рабочая станция №1, ул. Сергея Есенина, д. 48 – рабочая станция №2	Инженер, Начальник центра печати, Специалист по доставке

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

2.5 Анализ организационных мер защиты ИСПДн

Описание (пример заполнения подраздела): В ходе проведения проверки наличия и полноты методической и организационно-распорядительной документации прямо или косвенно относящейся к защите персональных данных было установлено, что документы по данной тематике не разрабатывались.

В зданиях, где находятся помещения ООО «Организация», все двери помещений оборудованы врезными замками. Доступ в помещения, где расположены рабочие станции, ограничен, войти могут только сотрудники.

Пожарная и охранная сигнализация установлена во всех помещениях, где обрабатываются персональные данные. Охрана объекта осуществляется частным охранным предприятием на договорной основе.

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

2.6 Анализ технологического процесса обработки информации, реализованного в информационной системе

Согласно представленному «Технологическому процессу обработки информации...» ИСПДн предназначена для обработки информации ограниченного доступа, формирования электронных документов (ЭД) и вывода их на печать. При этом информация в ИСПДн может поступать из других подразделений и организаций на учтенных бумажных или электронных носителях информации.

Для осуществления технологического процесса обработки информации в ИСПДн используется программное обеспечение (ПО), перечисленное в таблице №2.

ИСПДн предназначена для работы в многопользовательском режиме, доступ исполнителей к работе осуществляется по утвержденному списку, пользователи имеют разные права доступа к информации, ИСПДн имеет подключения к открытым информационным системам, передача персональных данных по открытым каналам связи осуществляется с использованием средств криптографической защиты.....

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

2.7 Результаты классификации ИСПДн ООО «Организация»

В соответствии с требованиями Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», выявлено, что тип актуальных угроз безопасности персональных данным ООО «Организация» относится к угрозам 3-го типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе…

В соответствии с требованиями Приказа ФСТЭК России от 18.02.2013г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» проведена классификация по уровням защищенности персональных данных при их обработке в информационных системах персональных данных в ООО «Организация», таблица 3.

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

2.7 Результаты классификации ИСПДн ООО «Организация»

Продолжение подраздела 2.7.

Таблица 3

№	Характеристика	Значение
1	Категория персональных данных	Иные категории ПДн
2	Субъекты ПДн	2.Не являются сотрудниками оператора
3	Объем обрабатываемых ПДн	до 100 000 субъектов ПДн
4	Тип актуальных угроз (на основании разработанной частной модели угроз и анализа актуальных угроз в ИСПДн)	Угрозы 3-го типа
5	Структура информационной системы	локальная информационная система
6	Подключение информационных систем к сетям общего пользования и (или) сетям международного информационного обмена	Имеется подключение к сети международного информационного обмена (СМИО) «Интернет»
7	Режим обработки персональных данных	Многопользовательский
8	Разграничению прав доступа пользователей	С разграничением прав доступа

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

2.7 Результаты классификации ИСПДн ООО «Организация»

Продолжение подраздела 2.7.

Таблица 3

№	Характеристика	Значение
1	Категория персональных данных	Иные категории ПДн
2	Субъекты ПДн	2.Не являются сотрудниками оператора
3	Объем обрабатываемых ПДн	до 100 000 субъектов ПДн
4	Тип актуальных угроз (на основании разработанной частной модели угроз и анализа актуальных угроз в ИСПДн)	Угрозы 3-го типа
5	Структура информационной системы	локальная информационная система
6	Подключение информационных систем к сетям общего пользования и (или) сетям международного информационного обмена	Имеется подключение к сети международного информационного обмена (СМИО) «Интернет»
7	Режим обработки персональных данных	Многопользовательский
8	Разграничению прав доступа пользователей	С разграничением прав доступа

По результатам анализа исходных данных информационной системы персональных данных, анализа актуальности угроз безопасности в разработанной частной модели угроз ООО «Организация», информационной системе персональных данных ООО «Организация» присвоен **4 уровень защищенности**.

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

К основным негативным последствиям от реализации угроз безопасности информации (УБИ) определено хищение денежных средств (рис. 3). Другие виды последствий также могут быть, но как правило они несут на несколько порядков меньший ущерб.

Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

Вид риска (ущерба)	Актуальность	Негативные последствия
У1 Ущерб физическому лицу	Отсутствует	
У2 Ущерб юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	Возможны	П2.2 Потеря (хищение) денежных средств
У3 Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	Отсутствует	

Рис. 3 – Возможные негативные последствия УБИ ООО «Организация»

4. Возможные объекты воздействия угроз безопасности информации

Актуальные объекты воздействия, интерфейсы доступа и возможные виды воздействия на них изображены на рис. 4.

Возможные объекты воздействия угроз безопасности информации

Негативные последствия	Наименование объекта воздействия	Интерфейсы доступа						Виды воздействия					
		ИНТ1	ИНТ2	ИНТ3	ИНТ4	ИНТ5	ИНТ6	В1	В2	В3	В4	В5	В6
П2.2	АРМ клиента ФО	да	да	да	да	да		да	да		да		
П2.2	Носитель информации				да			да	да		да		
П2.2	ПО клиентской части VPN или драйвера СКЗИ			да		да			да				
П2.2	Точка беспроводного доступа		да	да		да		да	да				
П2.2	Каналы связи						да	да	да				
П2.2	Системное программное обеспечение	да	да	да	да	да			да		да		
П2.2	Прикладное программное обеспечение	да	да	да	да	да	да	да	да		да		
П2.2	Платежная / финансовая информация			да				да	да		да		
П2.2	Учетные данные пользователя / ключи ЭП			да	да	да		да	да		да		

Рис. 4 – Возможные объекты воздействия УБИ ООО «Организация»

4. Возможные объекты воздействия угроз безопасности информации

Таблица 4 – Расшифровка интерфейсов доступа (для Н1, Н2)

Доступные интерфейсы	Шифр
Доступ через локальную вычислительную сеть организации	ИНТ1
Съемные машинные носители информации, подключаемые к АРМ пользователя	ИНТ2
Веб-интерфейс пользователя веб-сайта государственных услуг	ИНТ3
Сетевые интерфейсы коммутатора сети, где расположен веб-сервер	ИНТ4
Локальная вычислительная сеть организации	ИНТ5
Веб-интерфейс системы администрирования веб-сайта портала государственных услуг	ИНТ6

Таблица 5 – Расшифровка видов воздействия (для У2)

Виды воздействия	Шифр
Несанкционированная подмена данных, содержащихся в реквизитах платежного поручения	В1
Несанкционированная модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора	В2
Модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора	В3
Подмена данных, содержащих реквизиты платежных поручений и другой платежной информации на АРМ главного бухгалтера	В4
Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации	В5
Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации	В6

5. Источники угроз безопасности информации

Актуальные цели нарушителей, возможные негативные последствия, вид нарушителя, его категория и возможности изображены на рис. 5.

Источники угроз безопасности информации

Негативные последствия	Вид актуального нарушителя	Цель нарушителя											Категория нарушителя	Уровень возможностей нарушителя
		Ц1	Ц2	Ц3	Ц4	Ц5	Ц6	Ц7	Ц8	Ц9	Ц10	Ц11	Ц12	
П2.2	Преступные группы (криминальные структуры)						да		да					Внешний	Н2
П2.2	Отдельные физические лица (хакеры)						да		да					Внешний	Н1
П2.2	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)						да					да		Внутренний	Н1
П2.2	Авторизованные пользователи систем и сетей						да		да			да		Внутренний	Н1
П2.2	Системные администраторы и администраторы безопасности						да		да			да		Внутренний	Н2

Рис. 5 – Возможные источники УБИ ООО «Организация»

5. Источники угроз безопасности информации

Таблица 6 – Расшифровка Целей нарушителя

Цели нарушителя	Шифр
Желание самореализоваться	Ц1
Любопытство или желание самореализации (подтверждение статуса).	Ц2
Месть за ранее совершенные действия	Ц3
Получение финансовой выгоды за счет кражи и коммерческой тайны	Ц4
Получение финансовой выгоды за счет кражи и продажи персональных данных граждан	Ц5
Получение финансовой или иной материальной выгоды.	Ц6
Передача информации о юридическом лице третьим лицам	Ц7
Получение конкурентных преимуществ	Ц8
Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства	Ц9
Получение финансовой выгоды за счет использования вычислительных мощностей серверов государственной информационной системы для майнинга криптовалюты	Ц10
Непреднамеренные, неосторожные или неквалифицированные действия	Ц11
Получение финансовой или иной материальной выгоды при вступлении в сговор с преступной группой)	Ц12

6. Способы реализации (возникновения) угроз безопасности информации

Исходя из объектов воздействия и доступных интерфейсов, для каждого вида нарушителя определены актуальные способы реализации УБИ (рис.6).

Способы реализации (возникновения) угроз безопасности информации

Вид актуального нарушителя	Категория нарушителя	Способ реализации / Доступный интерфейс											
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
Преступные группы (криминальные структуры)	Внешний	1, 2, 3, 4, 5	1, 2, 3, 4, 5, 6			1, 4							
Отдельные физические лица (хакеры)	Внешний	1, 2, 3, 4, 5	1, 2, 3, 4, 5, 6										
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний		1, 2, 3, 4, 5, 6							1, 2, 3, 4, 5, 6	3	4,5,6	
Авторизованные пользователи систем и сетей	Внутренний		1, 2, 3, 4, 5, 6							1, 2, 3, 4, 5, 6	3	4,5,6	
Системные администраторы и администраторы безопасности	Внутренний	1, 2, 3, 4, 5	1, 2, 3, 4, 5, 6			1, 4			5, 6	1, 2, 3, 4, 5, 6	3	4,5,6	

Рис. 6 – Способы реализации УБИ ООО «Организация»

6. Способы реализации (возникновения) угроз безопасности информации

Таблица 7 – Расшифровка способов реализации

Способы реализации	Шифр
Использование недекларированных возможностей программного обеспечения телекоммуникационного оборудования	С1
Использование уязвимостей конфигурации системы управления базами данных	С2
Установка программных закладок в телекоммуникационное оборудование	С3
Использование уязвимостей кода коммутационного контроллера	С4
Извлечение аутентификационной информации из постоянной памяти носителя (инвазивный метод)	С5
Внедрение вредоносного программного обеспечения	С6
Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя	С7
Использование уязвимостей кода программного обеспечения веб-сервера	С8
Внедрение вредоносного кода в веб-приложение	С9
Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя	С10
Ошибочные действия в ходе настройки АРМ главного бухгалтера	С11
Нарушение цепочки услуг по администрированию портала государственных услуг	С12

7. Актуальные угрозы безопасности информации

7.1 Актуальные техники и тактики реализации угроз

Из общего состава техник и тактик, приведенных в Методике, исключаем те, которые не связаны с используемыми у нас технологиями, не применимы к нашим процессам, не приводящие к ущербу или недоступные актуальным нарушителям. Все актуальные сценарии должны быть подмножествами их этого ограниченного набора тактик (рис. 7.)

Рис.7

7. Актуальные угрозы безопасности информации

7.1 Актуальные техники и тактики реализации угроз

Таблица 7 – Расшифровка актуальных техник и тактик реализации УБИ

№	Тактика	Основные техники
T1	Сбор информации о системах и сетях Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации	T1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
		T1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: использование поисковой системы Shodan для получения информации об определенных моделях IP-камер видеонаблюдения с возможно уязвимыми версиями прошивок
		T1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей
		T1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: сканирование при помощи сканера nmap

7. Актуальные угрозы безопасности информации

7.1 Актуальные техники и тактики реализации угроз

Продолжение таблицы 7

T9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз Тактическая задача: в ходе реализации угроз безопасности информации, нарушителю может потребоваться получить и вывести за пределы инфраструктуры большие объемы информации, избежав при этом обнаружения или противодействия	T9.1. Доступ к системе для сбора информации и вывод информации через стандартные протоколы управления (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования. Пример: использование средств удаленного управления RMS / teamviewer для создания канала связи и управления скомпрометированной системой со стороны злоумышленников
		T9.2. Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы
		T9.3. Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
		T9.4. Вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
		T9.5. Отправка данных по известным протоколам управления и передачи данных
T10	Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям Тактическая задача: достижение нарушителем конечной цели, приводящее к реализации моделируемой угрозы и причинению недопустимых негативных последствий	T10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках
		T10.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа
		T10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения

7. Актуальные угрозы безопасности информации

7.2 Перечень актуальных угроз безопасности информации

Далее уже исходя из этих применимых тактик, возможностей нарушителей, объектов воздействия и их интерфейсов и способов реализации определены актуальные угрозы (рис. 8).

Актуальные угрозы безопасности информации

Группа актуальных угроз	Уровень возможностей нарушителей	Объекты воздействия	Способы реализации	Негативные последствия
Угрозы внедрения вредоносного кода	Н2	ПО клиентской части VPN или драйвера СКЗИ, Системное программное обеспечение, Прикладное программное обеспечение, Платежная / финансовая информация	С1, С2, С4, С5, С8, С9	П2.2
Угрозы воздействия на BIOS/UEFI	Н2	АРМ клиента ФО	С1, С2, С8, С10, С11	П2.2
Угрозы атаки на клиентов беспроводной сети	Н2	Точка беспроводного доступа	С1, С12	П2.2
Угрозы несанкционированной модификации защищаемой информации	Н2	Прикладное программное обеспечение, Платежная / финансовая информация	С1, С10, С12	П2.2
Угрозы внесения несанкционированных изменений в конфигурацию защищаемой системы	Н2	ПО клиентской части VPN или драйвера СКЗИ, Системное программное обеспечение, Прикладное программное обеспечение	С1, С2, С10	П2.2
Угрозы внесения несанкционированных изменений в прокладное программное обеспечение	Н2	Прикладное программное обеспечение	С1, С2, С10	П2.2
Угрозы изменения конфигурации сети	Н2	Системное программное обеспечение	С1, С12	П2.2
Угрозы несанкционированного доступа к аутентификационной информации	Н2	Учетные данные пользователя / ключи ЭП	С1, С2, С10, С11, С12	П2.2
Угрозы сбора информации о защищаемой системе	Н2	АРМ клиента ФО, ПО клиентской части VPN или драйвера СКЗИ, Каналы связи, Системное программное обеспечение, Прикладное программное обеспечение	С1, С10, С12	П2.2
Угрозы повышения привилегий	Н2	Системное программное обеспечение	С1, С2	П2.2
Угрозы подмены доверенных пользователей	Н2	Прикладное программное обеспечение	С1, С2, С10	П2.2
Угрозы ошибочных действий	Н2	Прикладное программное обеспечение	С9	П2.2

Рис. 8 – Актуальные УБИ ООО «Организация»

Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

ФИЛЬТРАЦИЯ

Контекстный поиск по названию угрозы

Введите слово или словосочетание

Источник угрозы

Доступен множественный выбор

Последствия реализации угрозы:

- Нарушение конфиденциальности
- Нарушение целостности
- Нарушение доступности

Сброс | Применить

Выводить по: 10, 20, 50, 100

Элементы с 1 по 10 из 207

УБИ. 001	Угроза автоматического распространения вредоносного кода в грид-системе
УБИ. 002	Угроза агрегирования данных, передаваемых в грид-системе
УБИ. 003	Угроза анализа криптографических алгоритмов и их реализации
УБИ. 004	Угроза аппаратного сброса пароля BIOS
УБИ. 005	Угроза внедрения вредоносного кода в BIOS
УБИ. 006	Угроза внедрения кода или данных
УБИ. 007	Угроза воздействия на программы с высокими привилегиями
УБИ. 008	Угроза восстановления аутентификационной информации
УБИ. 009	Угроза восстановления предыдущей уязвимой версии BIOS
УБИ. 010	Угроза выхода процесса за пределы виртуальной машины

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

30.10.2017
УБИ. 207 Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)

30.10.2017
УБИ. 206 Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем

01.09.2017
УБИ. 205 Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты

01.09.2017
УБИ. 204 Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров

01.09.2017
УБИ. 203 Угроза утечки информации с неподключенных к сети Интернет компьютеров

Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

ФИЛЬТРАЦИЯ

Контекстный поиск по названию уязвимости

Введите слово или словосочетание

Производитель ПО

Выберите производителя ПО

Тип ПО

Выберите тип ПО

Программное обеспечение

Выберите программное обеспе...

Аппаратная платформа

Выберите платформу

Версия ПО

Выберите версию ПО

Статус уязвимости

Выберите статус уязвимости

Доп. параметры

Диапазон дат

с

по

Выводить по: 10, 20, 50, 100 Сортировка:

Элементы с 1 по 10 из 17975

BDU:2018-00120	Уязвимость менеджера лицензий Sentinel License Manager, связанная с некорректным ограничением имени пути к каталогу, позволяющая нарушителю удалять или редактировать защищаемые файлы Gemalto N.V. Sentinel License Manager 18.01.55505	16.06.2016
BDU:2018-00119	Уязвимость платформы для защиты и лицензирования программного обеспечения Sentinel LDK RTE, вызванная выходом операции за границы буфера в памяти, позволяющая нарушителю вызвать отказ в обслуживании Gemalto N.V. Sentinel LDK RTE до 7.50 включительно	02.10.2017
BDU:2018-00118	Уязвимость функции cgiHandler веб-сервера Embedthis GoAhead, позволяющая нарушителю выполнить произвольный код Embedthis Software Embedthis GoAhead до 3.6.5	08.06.2017
BDU:2018-00117	Уязвимость функции auth_password службы sshd средства криптографической защиты OpenSSH, позволяющая нарушителю вызвать отказ в обслуживании OpenSSL Software Foundation OpenSSL до 7.2 включительно	21.07.2016
BDU:2018-00116	Уязвимость среды разработки CX-Programmer и микропрограммного обеспечения ПЛК Omron CJ2M и Omron CJ2H, связанная с обратимостью метода кодирования пароля, позволяющая нарушителю получить пароль доступа к контроллеру Omron Electronics LLC Omron CX-Programmer до 9.6	01.10.2015

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

25.01.2018
Уязвимость менеджера лицензий Sentinel License Manager, связанная с некорректным ограничением имени пути к каталогу, позволяющая нарушителю удалять или редактировать защищаемые файлы

25.01.2018
Уязвимость платформы для защиты и лицензирования программного обеспечения Sentinel LDK RTE, вызванная выходом операции за границы буфера в памяти, позволяющая нарушителю вызвать отказ в обслуживании

25.01.2018
Уязвимость функции cgiHandler веб-сервера Embedthis GoAhead, позволяющая нарушителю выполнить произвольный код

25.01.2018
Уязвимость функции auth_password службы sshd средства криптографической защиты OpenSSH, позволяющая нарушителю вызвать отказ в обслуживании

Окончание Модели угроз безопасности персональных данных, обрабатываемых в ИСПДн

Таким образом, в отношении персональных данных, обрабатываемых в ИСПДн ООО «Организация», актуальными являются следующие угрозы безопасности:

- угрозы внедрения вредоносного кода;
- угрозы воздействия на BIOS\UEFI;
- угрозы атаки на клиентов беспроводной сети;
- угрозы несанкционированной модификации защищаемой информации;
- угрозы внесения несанкционированных изменений в прикладное программное обеспечение;
- угрозы изменения конфигурации сети;
- угрозы несанкционированного доступа к аутентификационной информации;
- угрозы сбора информации о защищаемой системе;
- угрозы повышения привилегий;
- угрозы подмены доверенных пользователей;
- угрозы ошибочных действий.

Экспертная группа:

Начальник отдела ИБ ООО «Организация»	Иванов И.И.
Начальник отдела аудита ФГУП «НПП «Бэтта»	Васильев Р.А.
Ведущий специалист по ТЗИ ФГУП «НПП «Бэтта»	Петров В.И.

УТВЕРЖДАЮ
Директор ООО «Организация»

Д.В. Гусев

«13» марта 2021г.

Модель угроз безопасности информации
ИСПДн ООО «Организация»

СОГЛАСОВАНО

_____
«____» _____ 202___ г.

СОГЛАСОВАНО

_____
«____» _____ 202___ г.

2021 г.

ПРИСТУПАЕМ!

Содержание

АКАДЕМИЯ АЙТИ
a Softline Company

Спасибо за внимание!

Центральный офис:
Москва, Варшавское шоссе 47, корп. 4, 10 этаж
Тел: +7 (495) 150-9600
e-mail: academy@academyit.ru
Сайт: academyit.ru