ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 78e5dd9a2074c2b7bdf2e4cbad3cc414c7cff575
Владелец: Бутенко Ольга Николаевна
Действителен: с 21.02.2022 до 20.02.2027

УТВЕРЖДАЮ
Директор
МБОУ "Гимназия №27" имени Героя Советского Союза В.Е. Смирнова»
_____ Бутенко О.Н.

«30» августа 2021 г.
М.П.

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ МБОУ «ГИМНАЗИЯ №27» ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА В.Е. СМИРНОВА»

Барнаул 2021

1. Обозначения и сокращения:

АРМ — Автоматизированное рабочее место;
ИСПДн — информационная система персональных данных;
ПДн — персональные данные;
УБПДн — угрозы безопасности персональных данных;
НСД — несанкционированный доступ;
ПЭМИН — побочные электромагнитные излучения и наводки.

2. Термины и определения

Персональные данные — любая информация относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, социальное, имущественное положение, образование профессия, доходы, другая информация.

Технические каналы утечки информации — совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми обрабатывается защищаемая информация.

Угрозы безопасности персональных данных — совокупность условий и факторов создающих, опасность несанкционированного, в том числе случайного доступа к персональным данным, результатом которого может стать уничтожение изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Побочные электромагнитные излучения и наводки — электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и электромагнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

3. Общие положения

Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова» (далее – модель угроз, модель) разработана во исполнение требований подпункта «а» пункта 12 «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781, в соответствии с требованиями методических документов Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.

Информационные системы персональных данных МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова» предназначены для обеспечения основной деятельности МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова».

Целью обеспечения безопасности персональных данных при их обработке в информационных системах МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова» является обеспечение состояния защищенности прав и свобод человека и гражданина при обработке его персональных данных в МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова», которые гарантирует федеральное законодательство.

Угрозы могут быть внешними или внутренними в зависимости от дислокации источников угроз вне или внутри контролируемой зоны охраняемых объектов МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова» соответственно.

При этом в случае обработки персональных данных (организации персонифицированного учета) в электронной форме должны обеспечиваться гарантии их достоверности и защиты от искажений и несанкционированного доступа.

Перечень угроз безопасности персональных данных МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова»:

- противоправное распространение персональных данных;
- несанкционированное использование персональных данных, порождающее юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
- несанкционированное блокирование персональных данных;
- несанкционированное уничтожение персональных данных;
- несанкционированное изменение персональных данных;
- неправомерный или случайный доступ к персональным данным;
- неправомерное копирование персональных данных;
- иные неправомерные действия.

Модель угроз безопасности персональных данных предназначена для разработки системы защиты информационных систем.

4. Возможные последствия нарушения безопасности персональных данных

Возможными последствиями нарушения безопасности персональных данных, обрабатываемых в МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова», являются:

- разглашение персональных данных граждан Российской Федерации и причинение им материального ущерба;
- причинение материального ущерба;

- вред репутации МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова» в обществе.

5. Объекты угроз

Объектами угроз в ИСПДн МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова», подлежащими защите, являются информационные ресурсы, содержащие персональные данные, корпоративная сеть передачи данных, информационные технологии, технические и программные средства, используемые для обработки персональных данных, аппаратные и программные средства защиты.

5.1. Основные ресурсы, содержащие персональные данные

Основными информационным системами персональных данных, обрабатывающими персональные данные являются:

- Региональная информационная система "Сетевой регион. Образование;
- РИС ГИА-9, РИС ГИА-11;
- ИС «1С. Предприятие»;
- ИС «ОК "Зарплата"»;
- ИС «СБИС»;
- ИС «Сбербанк Онлайн»;
- ИС «СУФД»;
- ИС «Контур. Эксперт»;
- ИС «ОК «2НДФЛ»

5.2. Информация, формируемая в процессе создания и обработки персональных данных, но не содержащая персональных данных

В процессе обработки персональных данных в АС МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова» осуществляется формирование информации, не являющейся персональными данными, но получение которой злоумышленником способствует получению им доступа к персональным данным. По этой причине к объектам угроз относится:

- ключевая, аутентифицирующая и парольная информация;
- криптографически опасная информация;
- конфигурационная и управляющая информация;
- информация в электронных журналах регистрации;
- остаточная информация на носителях информации;
- информация, подверженная съему по побочному электромагнитному излучению и наводкам.

6. Основные угрозы безопасности персональных данных

Основными угрозами безопасности персональных данных является нарушение их конфиденциальности, целостности доступности и аутентичности.

Формирование Модели угроз осуществлено на основе определенных ранее угроз безопасности персональных данных при их обработке. Проведен анализ перечня угроз безопасности персональных данных с учетом оперативной обстановки, складывающейся вокруг МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова», имеющихся доступных материалов о реально зафиксированных угрозах безопасности персональных данных, а также имеющемся на общедоступном рынке средств защиты и средств технической разведки в информационной сфере.

При этом были выполнены требования нормативных правовых актов и учтены положения методических документов Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю.

Перечень и актуальность угроз безопасности персональных данных сформирован исходя из Модели нарушителя безопасности персональных данных МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова», анализа непреднамеренных (ошибочных, случайных) действий персонала МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова», учета условий жизнеобеспечения и системы энергоснабжения автоматизированной системы, а также влияния иных техногенных и природных факторов (стихийные бедствия и т.п.) (Таблица 1).

6.1. Основные формы реализации угроз конфиденциальности

Основными формами реализации угроз конфиденциальности персональных данных являются:

- визуальный съем отображаемой информации;
- подслушивание
- вредоносная программа;
- вторжение в ИСПД по информационно-телекоммуникационным сетям;
- закладка аппаратная;
- закладка программная;
- произвольное копирование баз данных (умышленные, в том числе злонамеренные, действия персонала);
- накопление данных пользователем ИСПД (умышленные действия персонала);
- накопление данных прикладными программами;
- неисправность аппаратных средств;
- ошибка в программе;
- ошибочные действия персонала;
- перехват в каналах передачи (телекоммуникационных сетях);
- произвольный доступ персонала системы к ресурсам;
- произвольное создание точек входа в ИСПД;

- утечка информации по побочному электромагнитному излучению и наводкам;
- хищение (утеря) или отчуждение носителей (модернизация, ремонт, утилизация).

6.2. Основные формы реализации угроз целостности

Основными формами реализации угроз целостности персональных данных являются:

- воздействие вредоносной программы;
- вторжение в ИСПД по информационно-телекоммуникационным сетям;
- закладка программная;
- злонамеренное разрушение, искажение персоналом (умышленные деструктивные действия персонала);
- искажение данных в каналах передачи (в информационно-телекоммуникационных сетях);
- нарушение энергоснабжения аппаратных средств ИСПД;
- неисправность аппаратных средств;
- ошибка в программе;
- ошибочные действия персонала;
- произвольное создание точек входа в ИСПД;
- стихийное бедствие, катастрофа.

6.3. Основные формы реализации угроз доступности

Основными формами реализации угроз доступности персональных данных являются:

- воздействие вредоносной программы;
- вторжение в ИСПД по информационно-телекоммуникационным сетям;
- закладка программная;
- злонамеренное блокирование данных персоналом (умышленные действия персонала);
- нарушение функционирования телекоммуникационных каналов;
- нарушение электроснабжения;
- неисправность аппаратных средств;
- несоответствие характеристик оборудования возложенным задачам;
- отказ систем жизнеобеспечения;
- ошибочные действия персонала;
- произвольное создание точек входа в ИСПД;
- стихийное бедствие, катастрофа.

6.4. Основные формы реализации угроз аутентичности

Основными формами реализации угроз аутентичности персональных данных являются:

вторжение в ИСПД по информационно-телекоммуникационным сетям;

фальсификация данных оператором (умышленные действия персонала).

7. Перечень актуальных угроз безопасности персональных данных

Перечень актуальных угроз разработан в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной заместителем директора Федеральной службы по техническому и экспортному контролю 14 февраля 2008 года.

7.1. Оценка уровня исходной защищенности информационных систем персональных данных.

Показатели исходной защищенности информационной системы персональных данных, влияющие на актуальность угроз безопасности персональных данных:

по территориальному признаку – локальная информационная система, развернутая в пределах одного здания (высокий уровень исходной защищенности);

по наличию соединений с сетями общего пользования – информационная система имеет многоточечный выход в телекоммуникационные сети общего пользования (низкий уровень исходной защищенности);

по встроенным (легальным) операциям с записями баз персональных данных – чтение, поиск, запись, удаление, сортировка, модификация, передача персональных данных (низкий уровень исходной защищенности);

по разграничению доступа к персональным данным – доступ имеет определенный приказами председателя МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова» перечень сотрудников (средний уровень исходной защищенности);

по наличию соединений с другими базами персональных данных других информационных систем персональных данных – в информационной системе используются только базы данных принадлежащие МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова» (высокий уровень исходной защищенности);

по уровню обобщения (обезличивания) персональных данных – предоставляемые пользователю данные не являются обезличенными (низкий уровень исходной защищенности);

по объему персональных данных, которые предоставляются сторонним пользователям информационной системы персональных данных – сторонним пользователям предоставляется часть персональных данных (средний уровень исходной защищенности).

Поскольку более 30% показателей исходной защищенности ИСПД имеют значение «низкий уровень исходной защищенности», то согласно раздела 2 «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» информационные системы персональных данных МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова» относится к информационным

системам с низкой степенью исходной защищенности и соответствующий числовой коэффициент (Y_1) равен 5.

7.2. Определение актуальности угроз безопасности персональных данных.

Актуальность угрозы в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» определяется с учетом оценок вероятности ее реализации и опасности.

блица 1

Перечень и актуальность угроз безопасности персональных данных

№	Форма реализации угрозы	Вероятность реализации угрозы (Y_2)	Интерпретация реализуемости угрозы $Y=(Y_1+Y_2)/20$	Опасность угрозы	Актуальность угрозы
1	Визуальный съём отображаемой информации:				
1.1	со средств отображения индивидуального пользования	высокая (10)	высокая (0,75)	низкая	актуальная
1.2	со средств коллективного отображения	низкая (2)	средняя (0,35)	низкая	неактуальная
1.3	с печатных документов	высокая (10)	высокая (0,75)	низкая	актуальная
2	Подслушивание	низкая (2)	средняя (0,35)	низкая	неактуальная
2	Вторжение в ИСПДн по информационно-телекоммуникационным сетям	высокая (10)	очень высокая (10)	высокая	актуальная
3	Воздействие вредоносной программы	высокая (10)	очень высокая (10)	высокая	актуальная
4	Закладки аппаратные	маловероятно (0)	низкая (0,25)	низкая	неактуальная
5	Закладки программные	маловероятно (0)	низкая (0,25)	низкая	неактуальная
6	Искажение в каналах передачи	маловероятно (0)	низкая (0,25)	низкая	неактуальная
7	Накопление данных прикладными программами	низкая (2)	средняя (0,35)	низкая	неактуальная
8	Нарушение функционирования телекоммуникационных каналов	низкая (2)	средняя (0,35)	низкая	неактуальная
9	Нарушение электроснабжения	низкая (2)	средняя (0,35)	низкая	неактуальная

№	Форма реализации угрозы	Вероятность реализации угрозы (Y_2)	Интерпретация реализуемости угрозы $Y=(Y_1+Y_2)/20$	Опасность угрозы	Актуальность угрозы
9.1	Внешнего	низкая (2)	средняя (0,35)	низкая	неактуальная
9.2	объектового	низкая (2)	средняя (0,35)	низкая	неактуальная
10	Неисправность аппаратных средств	низкая (2)	средняя (0,35)	низкая	неактуальная
11	Случаи несоответствия характеристик оборудования возложенным задачам	низкая (2)	средняя (0,35)	низкая	неактуальная
12	Отказ систем жизнеобеспечения	низкая (2)	средняя (0,35)	низкая	неактуальная
13	Ошибка в программе	низкая (2)	средняя (0,35)	средняя	актуальная
14	Ошибочные действия персонала	низкая (2)	средняя (0,35)	средняя	актуальная
15	Перехват в каналах передачи (телекоммуникационных сетях)	средняя (5)	средняя (0,5)	средняя	актуальная
16	Произвольное создание точек входа в систему за счет неправомерных действий	низкая (2)	средняя (0,35)	низкая	неактуальная
17	Несанкционированный доступ персонала ИС к ресурсам	низкая (2)	средняя (0,35)	средняя	актуальная
18	Стихийное бедствие, катастрофа	маловероятно (0)	низкая (0,25)	высокая	актуальная
19	Умышленные деструктивные действия персонала:				
19.1	произвольное копирование баз данных	средняя (5)	средняя (0,5)	средняя	актуальная
19.2	накопление данных пользователем информационной системы	средняя (5)	средняя (0,5)	средняя	актуальная
19.3	злонамеренное разрушение (искажение) информации	низкая (2)	средняя (0,35)	низкая	неактуальная
19.4	злонамеренное блокирование данных	низкая (2)	средняя (0,35)	низкая	неактуальная
19.5	фальсификация данных	низкая (2)	средняя (0,35)	низкая	неактуальная
20	Утечка данных по ПЭМИН	низкая (2)	средняя (0,35)	низкая	неактуальная
21	Хищение (утрата) или отчуждение машинных носителей	высокая (10)	очень высокая (10)	высокая	актуальная
22	Электромагнитное навязывание на элементы ИСПД (преднамеренное)	маловероятно (0)	низкая (0,25)	низкая	неактуальная

№	Форма реализации угрозы	Вероятность реализации угрозы (Y_2)	Интерпретация реализуемости угрозы $Y=(Y_1+Y_2)/2$ 0	Опасность угрозы	Актуальность угрозы
23	Преодоление (взлом) системы защиты персональных данных:				
23.1	компрометация аутентификатора;	низкая (2)	средняя (0,35)	средняя	актуальная
23.2	компрометация ключа СКЗИ;	маловероятно (0)	низкая (0,25)	низкая	неактуальная
23.3	нарушение функционирования средства защиты;	маловероятно (0)	низкая (0,25)	низкая	неактуальная
23.4	ошибка оператора средства защиты.	низкая (2)	средняя (0,35)	средняя	актуальная

8. Заключение

1. Информационные системы обработки персональных данных МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова» являются типовыми.

3. Нарушители безопасности персональных данных, обрабатываемых МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова», описываются в модели нарушителя.

4. Модель угроз должна быть методологической основой для разработки (при необходимости) частных (конкретизированных) моделей угроз для компонентов ИСПДн МБОУ «Гимназия №27» имени Героя Советского Союза В.Е. Смирнова».