**ПРАВИТЕЛЬСТВО АРХАНГЕЛЬСКОЙ ОБЛАСТИ**

# П О С Т А Н О В Л Е Н И Е

от 6 ноября 2018 г. № 523-пп

г. Архангельск

## Об утверждении Положения по определению угроз безопасности персональных данных, актуальных при их обработке в информационных системах персональных данных в исполнительных органах государственной власти Архангельской области, подведомственных им государственных учреждениях Архангельской области

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», в целях обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при их обработке в информационных системах персональных данных в исполнительных органах государственной власти Архангельской области, подведомственных им государственных учреждениях Архангельской области, Правительство Архангельской области **п о с т а н о в л я е т**:

1. Утвердить прилагаемое Положение по определению угроз безопасности персональных данных, актуальных при их обработке в информационных системах персональных данных в исполнительных органах государственной власти Архангельской области, подведомственных им государственных учреждениях Архангельской области (далее – Положение).

2. Исполнительным органам государственной власти Архангельской области, подведомственным им государственным учреждениям Архангельской области при разработке частных моделей угроз учитывать актуальные угрозы, указанные в Положении.

3. Рекомендовать органам местного самоуправления муниципальных образований Архангельской области, подведомственным им муниципальным учреждениям руководствоваться Положением при определении угроз безопасности персональных данных, актуальных при обработке персональных

данных в используемых ими информационных системах персональных данных.

4. Настоящее постановление вступает в силу со дня его официального опубликования.

**Первый заместитель Губернатора Архангельской области – председатель Правительства Архангельской области**  **А.В. Алсуфьев**

УТВЕРЖДЕНО
постановлением Правительства
Архангельской области
от 6 ноября 2018 г. № 523-пп

# П О Л О Ж Е Н И Е
# по определению угроз безопасности персональных данных, актуальных при их обработке в информационных системах персональных данных в исполнительных органах государственной власти Архангельской области, подведомственных им государственных учреждениях Архангельской области

## I. Общие положения

1. Настоящее Положение, разработанное в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), определяет угрозы безопасности персональных данных (далее – ПДн), актуальные при обработке ПДн в информационных системах (далее – ИС) ПДн (далее – ИСПДн) в исполнительных органах государственной власти Архангельской области, подведомственных им государственных учреждениях Архангельской области (далее – государственные органы).

2. Угрозы безопасности ПДн, обрабатываемых в ИСПДн, приведенные в настоящем Положении, подлежат изменению и адаптации в ходе разработки операторами ИСПДн частных моделей угроз безопасности информации. В процессе этой работы проводится анализ структурно-функциональных характеристик конкретной ИСПДн, применяемых в ней информационных технологий и особенностей ее функционирования. По результатам анализа делается вывод об отнесении ИСПДн к одному из видов ИСПДн, указанных в пункте 5 настоящего Положения.

## II. Порядок определения актуальных угроз

3. В частной модели угроз безопасности информации указываются:

1) описание ИСПДн и ее структурно-функциональных характеристик;

2) описание угроз безопасности информации, включающее описание возможностей нарушителя (модель нарушителя), возможных уязвимостей ИС, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

4. Актуальные угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в настоящем Положении, изменяются по мере выявления новых источников угроз, развития способов и средств реализации угроз

безопасности ПДн в ИСПДн. Изменения, указанные в пункте 2 настоящего Положения, согласовываются с Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) и Федеральной службой безопасности Российской Федерации в соответствии с пунктом 3 требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 6 июля 2015 года № 676.

5. В государственных органах создаются и эксплуатируются однотипные и разноплановые ИСПДн. В зависимости от предназначения ИСПДн подразделяются:

1) на ИСПДн обеспечения типовой деятельности, предназначенные для автоматизации обеспечивающей деятельности государственных органов в рамках исполнения ими типовых полномочий, предусмотренных нормативными правовыми актами.

К ИСПДн обеспечения типовой деятельности относятся:

а) ИСПДн управления персоналом (учет кадров);

б) ИСПДн управления финансами (расчет заработной платы);

2) на ИСПДн обеспечения специальной деятельности, предназначенные для автоматизации или информационной поддержки предоставления государственных услуг, исполнения государственных функций, предусмотренных нормативными правовыми актами Архангельской области в качестве полномочий конкретного государственного органа. К ИСПДн обеспечения специальной деятельности относятся:

а) «Система электронного документооборота Правительства Архангельской области «Дело»;

б) «Региональная система межведомственного электронного взаимодействия Архангельской области»;

в) «Комплексная информационно-аналитическая система Архангельской области»;

3) ИСПДн по направлениям деятельности государственных органов, предназначенные для предоставления государственных услуг, исполнения государственных функций.

## III. Объекты защиты ИСПДн, классификация и характеристики нарушителей

6. В системе защиты информации ИСПДн к объектам защиты относятся:

1) персональные данные – объект 1;

2) средства криптографической защиты информации (далее – СКЗИ) – объект 2;

3) среда функционирования средств защиты информации, в том числе СКЗИ (далее – СФ), – объект 3;

4) информация, относящаяся к криптографической защите ПДн, включая ключевую, парольную и аутентифицирующую информацию СКЗИ, – объект 4;

5) документы, включая документацию на СКЗИ и на технические и программные компоненты СФ, – объект 5;

6) носители защищаемой информации, используемые в ИСПДн в процессе криптографической защиты ПДн, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним – объект 6;

7) каналы (линии) связи, используемые информационной системой, – объект 7;

8) помещения, в которых находятся ресурсы ИС, имеющие отношение к криптографической защите ПДн, – объект 8.

7. По наличию права постоянного или разового доступа в контролируемую зону ИСПДн нарушители подразделяются на два типа:

внешние нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

внутренние нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн.

8. Внешними нарушителями могут быть:

разведывательные службы иностранных государств;

юридические лица;

физические лица.

9. Внешний нарушитель имеет возможность осуществлять:

несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;

несанкционированный доступ через автоматизированное рабочее место (далее – АРМ), подключенное к сетям связи общего пользования и (или) к сетям международного информационного обмена;

несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;

несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;

несанкционированный доступ через ИС взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

10. Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн:

1) к первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.

Лицо этой категории может:

иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;

располагать фрагментами информации о топологии ИСПДн и об используемых коммуникационных протоколах и их сервисах;

располагать именами и вести выявление паролей зарегистрированных пользователей;

изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн;

2) ко второй категории относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.

Лицо этой категории:

обладает всеми возможностями лиц первой категории;

знает одно и более рабочее имя доступа;

обладает всеми необходимыми атрибутами, обеспечивающими доступ к некоторому подмножеству ПДн;

располагает конфиденциальными данными, к которым имеет доступ;

3) к третьей категории относятся зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным ИС.

Лицо этой категории:

обладает всеми возможностями лиц первой и второй категорий;

располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной ИС, через которую осуществляется доступ, и о составе технических средств ИСПДн;

имеет возможность физического доступа к фрагментам технических средств ИСПДн;

4) к четвертой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента ИСПДн.

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте ИСПДн;

обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;

имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте ИСПДн;

имеет доступ ко всем техническим средствам сегмента ИСПДн;

обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн;

5) к пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

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;

6) к шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

обладает полной информацией об ИСПДн;

имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

не имеет прав доступа к конфигурированию технических средств сети, за исключением контрольных (инспекционных);

7) к седьмой категории относятся программисты-разработчики прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

Лицо этой категории:

обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение (далее – ПО) ИСПДн на стадии ее разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн;

8) к восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств ИСПДн.

Лицо этой категории:

обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

11. Возможность или невозможность доступа каждой категории нарушителей к объектам защиты определяется в соответствии с таблицей № 1.

Таблица № 1

| Объект защиты | I категория наруши-телей | II категория наруши-телей | III категория наруши-телей | IV категория наруши-телей | V категория наруши-телей | VI категория наруши-телей | VII категория наруши-телей | VIII категория наруши-телей |
|---|---|---|---|---|---|---|---|---|
| Объект 1 | нет доступа | есть доступ | есть доступ | есть доступ | есть доступ | нет доступа | нет доступа | нет доступа |
| Объект 2 | есть доступ | есть доступ | есть доступ | есть доступ | есть доступ | есть доступ | нет доступа | есть доступ |
| Объект 3 | есть доступ | есть доступ | есть доступ | есть доступ | есть доступ | есть доступ | нет доступа | есть доступ |
| Объект 4 | есть доступ | есть доступ | есть доступ | есть доступ | есть доступ | есть доступ | нет доступа | нет доступа |
| Объект 5 | есть доступ | нет доступа | нет доступа | нет доступа | нет доступа | есть доступ | нет доступа | есть доступ |
| Объект 6 | есть доступ | нет доступа | нет доступа | есть доступ | есть доступ | есть доступ | нет доступа | нет доступа |
| Объект 7 | есть доступ | нет доступа | есть доступ | есть доступ | есть доступ | есть доступ | нет доступа | нет доступа |
| Объект 8 | есть доступ | есть доступ | есть доступ | есть доступ | есть доступ | есть доступ | нет доступа | есть доступ |

12. Источники атак на объекты ИСПДн располагают обобщенными возможностями в соответствии с таблицей № 2.

Таблица № 2

| № п/п | Обобщенные возможности источников атак | Да/нет |
|---|---|---|
| 1. | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны (далее – КЗ) | да |
| 2. | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах КЗ, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования | да |
| 3. | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах КЗ 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 ПО) | 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 |

13. Уточненные возможности нарушителей и направления атак приведены в таблице № 3.

Таблица № 3

| № п/п | Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы) | Актуальность использования (применения) угроз для построения и реализации атак | Обоснование отсутствия актуальных угроз безопасности |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 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;<br>высокая стоимость и сложность подготовки реализации возможности;<br>проводятся работы по подбору персонала;<br>доступ в КЗ и помещения, где располагаются средства вычислительной техники (далее – СВТ), на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;<br>помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;<br>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 сотрудников по эксплуатации;<br>осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;<br>осуществляется регистрация и учет действий пользователей;<br>на АРМ и серверах, на которых установлены СКЗИ, используются: |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | | | сертифицированные средства защиты информации от несанкционированного доступа;<br>сертифицированные средства антивирусной защиты |
| 2. | Проведение лабораторных исследований СКЗИ, используемых вне КЗ, ограниченное мерами, реализованными в ИС, 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;<br>высокая стоимость и сложность подготовки реализации возможности |
| 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;<br>высокая стоимость и сложность подготовки реализации возможности |
| 4. | 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;<br>высокая стоимость и сложность подготовки реализации возможности;<br>проводятся работы по подбору персонала;<br>доступ в КЗ и помещения, где располагаются СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;<br>помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок |

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| | | | и их открытие только для санкционированного прохода;<br>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 сотрудников по эксплуатации;<br>осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;<br>осуществляется регистрация и учет действий пользователей;<br>на АРМ и серверах, на которых установлены СКЗИ, используются: сертифицированные средства защиты информации от несанкционированного доступа;<br>сертифицированные средства антивирусной защиты |
| 5. | 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 |
| 6. | Возможность воздействовать на любые компоненты СКЗИ и СФ | не актуально | не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности |

## III. Актуальные угрозы безопасности

14. Учитывая особенности обработки ПДн в государственных органах, а также категорию и объем обрабатываемых в ИСПДн ПДн, основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность – обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

Целостность – состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

Доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

15. Под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в ИС, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия. Для определения актуальных угроз безопасности из общего перечня угроз безопасности выбираются только те угрозы, которые являются актуальными для ИСПДн обеспечения типовой или специальной деятельности.

16. Угрозы безопасности ПДн, актуальные при обработке ПДн в ИСПДн, подразделяются на угрозы первого, второго, третьего типа. Для определения актуальных угроз безопасности из общего перечня угроз безопасности выбираются только те угрозы, которые являются актуальными для ИСПДн в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14 февраля 2008 года. Большинство угроз безопасности ПДн в ИСПДн государственных органов относится к третьему типу. Уровень защищенности ПДн в ИСПДн государственных органов – не выше третьего уровня защищенности (за исключением ИС регионального масштаба, обрабатывающих специальные категории ПДн).

17. Основной целью применения СКЗИ в ИСПДн государственных органов является защита ПДн при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию.

18. В ИСПДн обеспечения типовой и специальной деятельности не используются отчуждаемые носители защищаемой информации, для которых несанкционированный доступ к хранимой на них информации не может быть исключен без использования криптографических методов и способов.

19. Основными видами угроз безопасности ПДн в ИСПДн являются:

а) угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);

б) угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель);

в) угрозы, возникновение которых напрямую зависит от свойств техники и ПО, используемого в ИСПДн;

г) угрозы, возникающие в результате внедрения аппаратных закладок и вредоносных программ;

д) угрозы, направленные на нарушение нормальной работы технических средств, используемых в ИСПДн;

е) угрозы, связанные с недостаточной квалификацией обслуживающего ИСПДн персонала.

20. Перечень актуальных и неактуальных угроз безопасности приведен в таблице № 4.

Таблица № 4

| № п/п | Наименование угрозы безопасности | Актуальность |
|---|---|---|
| 1 | 2 | 3 |
| 1. | Угрозы утечки по техническим каналам | |
| 1.1. | Угрозы утечки акустической информации | не актуально |
| 1.2. | Угрозы утечки видовой информации | не актуально |
| 1.3. | Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок | не актуально |
| 2. | Угрозы несанкционированного доступа к информации | |
| 2.1. | Угрозы уничтожения, хищения АС ИСПДн носителей информации путем физического доступа к элементам ИСПДн | |
| 2.1.1. | Кража персональной электронно-вычислительной машины (далее – ПЭВМ) | не актуально |
| 2.1.2. | Кража носителей информации | актуально |
| 2.1.3. | Кража ключей и атрибутов доступа | актуально |
| 2.1.4. | Кражи, модификации, уничтожения информации | не актуально |
| 2.1.5. | Вывод из строя узлов ПЭВМ, каналов связи | актуально |
| 2.2. | Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (далее – НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий) | |
| 2.2.1. | Действия вредоносных программ (вирусов) | не актуально |
| 2.2.2. | Недекларированные возможности системного ПО и ПО для обработки ПДн | не актуально |
| 2.2.3. | Установка ПО, не связанного с исполнением служебных обязанностей | не актуально |
| 2.3. | Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты ПДн в ее составе из-за сбоев в ПО, а также от угроз неантропогенного (сбой аппаратуры из-за ненадежности элементов, сбой электропитания) и стихийного (удары молний, пожары, наводнения и т.п.) характера | |
| 2.3.1. | Утрата ключей и атрибутов доступа | актуально |
| 2.3.2. | Непреднамеренная модификация (уничтожение) информации сотрудниками | не актуально |
| 2.3.3. | Непреднамеренное отключение средств защиты | актуально |
| 2.3.4. | Выход из строя аппаратно-программных средств | актуально |

| 1 | 2 | 3 |
|---|---|---|
| 2.3.5. | Сбой системы электроснабжения | не актуально |
| 2.3.6. | Стихийное бедствие | не актуально |
| 2.4. | Угрозы преднамеренных действий внутренних нарушителей | |
| 2.4.1. | Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке | не актуально |
| 2.4.2. | Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке | актуально |

21. В случае подключения ИСПДн к локальным вычислительным сетям, имеющим подключения к сетям общего пользования и (или) сетям международного информационного обмена, актуальными и неактуальными являются дополнительные угрозы безопасности, указанные в таблице № 5.

Таблица № 5

| **№ п/п** | **Наименование угрозы безопасности** | **Актуальность** |
|---|---|---|
| 1 | 2 | 3 |
| 1. | Угрозы несанкционированного доступа по каналам связи | |
| 1.1. | Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации | актуально |
| 1.2. | Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений | актуально |
| 1.3. | Угрозы выявления паролей по сети | актуально |
| 1.4. | Угрозы навязывания ложного маршрута сети | актуально |
| 1.5. | Угрозы подмены доверенного объекта в сети | актуально |
| 1.6. | Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | актуально |
| 1.7. | Угрозы типа «Отказ в обслуживании» | актуально |
| 1.8. | Угрозы удаленного запуска приложений | актуально |
| 1.9. | Угрозы внедрения по сети вредоносных программ | актуально |
| 2. | Угрозы среды виртуализации | |
| 2.1. | Совершение атаки с виртуальной машины на другую виртуальную машину | актуально |
| 2.2. | Совершение атаки на систему управления виртуальной инфраструктурой | актуально |
| 2.3. | Совершение атаки на монитор виртуальных машин из физической сети | не актуально |
| 2.4. | Нарушение процедуры аутентификации субъектов виртуализированного информационного взаимодействия | не актуально |
| 2.5. | Нарушение работоспособности ИС, построенных на основе технологии виртуализации, за счет несанкционированного доступа к средствам виртуализации | не актуально |
| 2.6. | Атака на виртуальные каналы передачи данных | не актуально |
| 2.7. | Несанкционированный доступ к образам виртуальных машин | не актуально |
| 2.8. | Нарушение изоляции пользовательских данных внутри виртуальных машин | не актуально |
| 2.9. | Атака на гипервизор с виртуальной машины | не актуально |

| 1 | 2 | 3 |
|---|---|---|
| 2.10. | Атака на гипервизор из физической среды | не актуально |
| 2.11. | Атака на защищаемые виртуальные машины из физической сети | не актуально |
| 2.12. | Неконтролируемый рост числа виртуальных машин | не актуально |
| 2.13. | Атака на сеть репликации виртуальных машин | не актуально |
| 2.14. | Выход процесса за пределы виртуальной среды | не актуально |

22. В случае использования для защиты персональных данных СКЗИ актуальными и неактуальными являются дополнительные угрозы безопасности, указанные в таблице № 6.

Таблица № 6

| **№ п/п** | **Наименование угрозы безопасности** | **Актуальность** |
|---|---|---|
| 1 | 2 | 3 |
| 1. | Угрозы безопасности ПДн при их обработке в ИС с использованием СКЗИ | |
| 1.1. | Подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ | актуально |
| 1.2. | Подготовка и проведение атак на этапах жизненного цикла СКЗИ: разработка (модернизация) СКЗИ, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы):<br>внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности представляющие СФ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;<br>внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ | не актуально |
| 1.3. | Проведение атаки нарушителем вне КЗ | актуально |
| 1.4. | Проведение атак на этапе эксплуатации СКЗИ:<br>на персональные данные;<br>на ключевую, аутентифицирующую и парольную информацию СКЗИ;<br>на программные компоненты СКЗИ;<br>на аппаратные компоненты СКЗИ;<br>на программные компоненты СФ, включая программное обеспечение BIOS;<br>на аппаратные компоненты СФ;<br>на данные, передаваемые по каналам связи | актуально |
| 1.5. | Получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об ИС, в которой используется СКЗИ | актуально |
| 1.6. | Применение:<br>находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;<br>специально разработанных АС и ПО | актуально |

| 1 | 2 | 3 |
|---|---|---|
| 1.7. | Использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:<br>каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;<br>каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ | актуально |
| 1.8. | Проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если ИС, в которых используются СКЗИ, имеют выход в эти сети | актуально |
| 1.9. | Использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ | актуально |
| 1.10. | Проведение атаки при нахождении в пределах КЗ | не актуально |
| 1.11. | Проведение атак на этапе эксплуатации СКЗИ на следующие объекты:<br>документацию на СКЗИ и компоненты СФ;<br>помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ | не актуально |
| 1.12. | Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:<br>сведений о физических мерах защиты объектов, в которых размещены ресурсы ИС;<br>сведений о мерах по обеспечению КЗ объектов, в которых размещены ресурсы ИС;<br>сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ | не актуально |
| 1.13. | Использование штатных средств, ограниченное мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий | не актуально |
| 1.14. | Использование физического доступа к СВТ, на которых реализованы СКЗИ и СФ | не актуально |
| 1.15. | Возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий | не актуально |
| 1.16. | 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 |
| 1.17. | Проведение лабораторных исследований СКЗИ, используемых вне КЗ, ограниченное мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий | не актуально |

| 1 | 2 | 3 |
|---|---|---|
| 1.18. | 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 |
| 1.19. | Проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО | не актуально |
| 1.20. | Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ | не актуально |
| 1.21. | Возможность располагать всеми аппаратными компонентами СКЗИ и СФ | не актуально |

23. Актуальные угрозы безопасности ИСПДн обеспечения типовой деятельности.

1) ИСПДн обеспечения типовой деятельности отличаются следующими особенностями:

использованием стандартных (унифицированных) технических средств обработки информации;

использованием типового ПО;

наличием незначительного количества АРМ, участвующих в обработке ПДн;

дублированием информации, содержащей ПДн, на бумажных носителях и на магнитных накопителях информации (далее – МНИ);

незначительными негативными последствиями для субъектов ПДн при реализации угроз безопасности ИСПДн;

эксплуатацией ИСПДн сотрудниками государственных органов без привлечения на постоянной основе сторонних организаций;

жесткой регламентацией процедуры взаимодействия со сторонними организациями (банки, пенсионные, страховые и налоговые органы, органы статистики);

2) актуальными угрозами безопасности ПДн в ИСПДн обеспечения типовой деятельности в государственных органах являются:

кража носителей информации;

кража ключей и атрибутов доступа;

вывод из строя узлов ПЭВМ, каналов связи;

несанкционированное отключение средств защиты;

утрата ключей и атрибутов доступа;

непреднамеренная модификация (уничтожение) информации сотрудниками;

непреднамеренное отключение средств защиты;

выход из строя аппаратно-программных средств;

разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

24. Актуальные угрозы безопасности ПДн в ИСПДн обеспечения специальной деятельности.

1) ИСПДн обеспечения специальной деятельности отличаются следующими особенностями:

использованием широкой номенклатуры технических средств получения, отображения и обработки информации;

использованием специального ПО;

наличием значительного количества АРМ, участвующих в обработке ПДн;

построением ИСПДн на базе распределенной по территории Архангельской области вычислительной сети со сложной архитектурой;

наличием подключений к сетям связи общего пользования и (или) международного информационного обмена;

использованием разнообразной телекоммуникационной инфраструктуры, принадлежащей различным операторам связи;

широким применением средств защиты информации, включая сертифицированные СКЗИ;

использованием аутсорсинга при создании и эксплуатации ИСПДн и ее элементов;

сложностью с дублированием больших массивов информации, содержащей ПДн, на бумажных носителях и МНИ;

значительными негативными последствиями при реализации угроз безопасности ИСПДн;

недостаточной квалификацией пользователей и обслуживающего ИСПДн и средства защиты информации персонала;

проблемами взаимодействия различных ИСПДн, вызванных несовершенством законодательства Российской Федерации;

2) актуальными угрозами безопасности ПДн в ИСПДн обеспечения специальной деятельности в государственных органах являются:

кража носителей информации;

кража ключей и атрибутов доступа;

вывод из строя узлов ПЭВМ, каналов связи;

несанкционированное отключение средств защиты;

утрата ключей и атрибутов доступа;

непреднамеренная модификация (уничтожение) информации сотрудниками;

непреднамеренное отключение средств защиты;

выход из строя аппаратно-программных средств;

разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке;

угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;

угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений;

угрозы выявления паролей по сети;

угрозы навязывания ложного маршрута сети;

угрозы подмены доверенного объекта в сети;

угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

угрозы типа «Отказ в обслуживании»;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ;

совершение атаки с виртуальной машины на другую виртуальную машину;

совершение атаки на систему управления виртуальной инфраструктурой;

подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

проведение атаки нарушителем вне КЗ;

проведение атак на этапе эксплуатации СКЗИ:

а) на персональные данные;

б) на ключевую, аутентифицирующую и парольную информацию СКЗИ;

в) на программные компоненты СКЗИ;

г) на аппаратные компоненты СКЗИ;

д) на программные компоненты СФ, включая программное обеспечение BIOS;

е) на аппаратные компоненты СФ;

ж) на данные, передаваемые по каналам связи;

получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об ИС, в которой используется СКЗИ;

применение:

а) находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;

б) специально разработанных АС и ПО;

использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:

а) каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;

б) каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если ИС, в которых используются СКЗИ, имеют выход в эти сети;

использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств ИС, применяемых на местах эксплуатации СКЗИ.