**Практическое задание №3.**

***1. Вопрос: В Вашей организации вводится в эксплуатацию государственная информационная система (ГИС). Кто по нормативным документам должен организовать разработку системы защиты информации информационной системы, а кто может проектировать и разрабатывать систему защиты информации ГИС? Приведите ссылку на пункт нормативного документа.***

**Ответ:** Согласно пункту 15 Приказа ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (далее – Приказ). Разработка системы защиты информации информационной системы **организуется** обладателем информации (заказчиком).

Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы с учетом ГОСТ 34.601 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания" (далее – ГОСТ 34.601), ГОСТ Р 51583 и ГОСТ Р 51624 и в том числе включает:

* проектирование системы защиты информации информационной системы;
* разработку эксплуатационной документации на систему защиты информации информационной системы;
* макетирование и тестирование системы защиты информации информационной системы (при необходимости).

Система защиты информации информационной системы не должна препятствовать достижению целей создания информационной системы и ее функционированию. При разработке системы защиты информации информационной системы учитывается ее информационное взаимодействие с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также применение вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

В соответствии с пунктом 10 Приказа. Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности" (Собрание законодательства Российской Федерации, 2011, N 19, ст. 2716; N 30, ст. 4590; N 43, ст. 5971; N 48, ст. 6728; 2012, N 26, ст. 3446; N 31, ст. 4322; 2013, N 9, ст. 874).

***2.Вопрос: Ваша организация эксплуатирует государственная информационная система (ГИС) 3 класса защищённости. Какие группы организационно-распорядительных документов по защите информации в вашей ГИС должны быть? На основании каких нормативных документов?***

**Ответ:** Согласно пункту 16.2 Приказа ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

* управления (администрирования) системой защиты информации информационной системы;
* выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;
* управления конфигурацией аттестованной информационной системы и системы защиты информации информационной системы;
* контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;
* защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

***3.Вопрос: В Вашей организации формируются требования для создания системы защиты государственной информационной системы (ГИС). По нормативным документам Вам необходимо разработать Модель угроз безопасности информации в ГИС. Что должна содержать Модель угроз безопасности информации? Приведите названия документов, необходимых для ее создания.***

**Ответ:** В соответствии пунктом 14.3 Приказа ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, 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 в соответствии с подпунктами 4 и 8 «Положения о Федеральной службе по техническому и экспортному контролю», утвержденного Указом Президента Российской Федерации от 16.08.2004 № 1085 (ред. от 13.06.2019).

***4.Вопрос: Нужно или нет согласовывать разработанные в федеральных органах исполнительной власти модель угроз безопасности информации и техническое задание на создание системы защиты для ГИС? Если необходимо, то на основании какого документа?***

**Ответ:** Постановлением Правительства Российской Федерации от 11.05.2017 № 555 внесены изменения в Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утверждённые постановлением Правительства Российской Федерации от 06.07.2015 № 676.

В соответствии с пунктом 3 указанных Требований модели угроз безопасности информации и \или технические задания на создание государственных информационных систем согласуются с ФСТЭК России в пределах ее полномочий в части выполнения установленных требований о защите информации.

Рассмотрение и согласование моделей угроз безопасности информации и технических заданий на создание федеральных информационных систем осуществляется центральным аппаратом ФСТЭК России. Рассмотрение и согласование моделей угроз безопасности информации и технических заданий на создание региональных информационных систем осуществляется

управлениями ФСТЭК России по федеральным округам.

Рассмотрению в ФСТЭК России подлежат проекты моделей угроз безопасности информации и технических заданий на создание государственных информационных систем, оформленные в установленном порядке и поступившие от заказчиков или операторов государственных информационных систем.

 ***5.Вопрос: В Вашей организации вводится в эксплуатацию иная (негосударственная) автоматизированная система, в которой обрабатывается коммерческая тайна, все рабочие места – многопользовательские и объединяются в локальную сеть, у всех пользователей – разные права
на доступ к информации. К какому классу защищённости от НСД должна быть отнесена Ваша АС? На основании каких документов ФСТЭК России?***

**Ответ:** В соответствии с Руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. Решением Гостехкомиссии России от 30.03.1992) и «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (утв. 30.08.2002 приказом Председателя Гостехкомиссии России № 282)»:

* первая группа включает многопользовательские автоматизированные системы, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А [п. 1.9 Руководящего документа];
* автоматизированная система, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Г [п. 5.2.3 СТР-К].
* Таким образом, вводимая в эксплуатацию автоматизированная система должна быть отнесена к классу защищённости от НСД **1Г.**

 ***6. Вопрос: В Вашей организации вводится в эксплуатацию иная (негосударственная) автоматизированная система, в которой обрабатывается открытая информация и информация для служебного пользования, все рабочие места – однопользовательские и объединяются в локальную сеть,
у всех пользователей – одинаковые права на доступ к информации. К какому классу защищённости от НСД должна быть отнесена Ваша АС? На основании каких документов ФСТЭК России?***

**Ответ:** В соответствии с Руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. Решением Гостехкомиссии России от 30.03.1992) и «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (утв. 30.08.2002 приказом Председателя Гостехкомиссии России № 282)» (далее – СТР-К):

* вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.
* автоматизированная система, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Г [пункт 5.2.3 СТР-К].

Таким образом, вводимая в эксплуатацию автоматизированная система должна быть отнесена к классу защищённости от **НСД 2Б.**

 ***7. Вопрос: Кто и по каким критериям присваивает класс защищённости для ГИС, эксплуатируемой в организации, органе государственной власти? На основании каких нормативных документов?***

**Ответ:** В соответствии Приказом ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – Требования) формирование требований к защите информации, содержащейся в государственной информационной системе, осуществляется обладателем информации (заказчиком), с учетом [ГОСТ-а Р 51583](http://login.consultant.ru/link/?req=doc;base=OTN;n=6914;fld=134) «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» и ГОСТ-а Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» и в том числе включает:

* принятие решения о необходимости защиты информации, содержащейся в информационной системе;
* классификацию информационной системы по требованиям защиты информации (далее – классификация информационной системы);
* определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;
* определение требований к системе защиты информации информационной системы [пункт 14 Требований].

Классификация информационной системы проводится в зависимости от:

* уровня значимости обрабатываемой в ней информации;
* масштаба информационной системы (федеральный, региональный, объектовый).

Устанавливаются три класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации (первый класс (К1), второй класс (К2), третий класс (К3)). Самый низкий класс – третий, самый высокий – первый.

Класс защищенности определяется для информационной системы в целом и, при необходимости, для ее отдельных сегментов (составных частей).

Результаты классификации информационной системы оформляются актом классификации [пункт 14.2 Требований].

 ***8. Вопрос: В Вашей организации вводится в эксплуатацию государственная информационная система, в которой обрабатывается информация для служебного пользования, уровень ИС – региональный, степень возможного ущерба от нарушения конфиденциальности информации – средняя, степень возможного ущерба от нарушения целостности и доступности информации - низкая. Какой уровень значимости и класс защищённости Вы присвоите данной ГИС? На основании какого нормативного документа?***

**Ответ:** В соответствии Приказом ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – Требования) информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба.

Воспользовавшись таблицей, приведенной в Приложении №1 Требований, можем определить класс защищенности.

Исходя из вышеизложенного и поставленного вопроса, данной государственной информационной системе необходимо присвоить уровень значимости – **УЗ 2** и класс защищенности – **К2**.

 ***9. Вопрос: В Вашей организации вводится в эксплуатацию государственная информационная система (ГИС), в которой обрабатываются персональные данные, уровень ГИС – объектовый, степень возможного ущерба
от нарушения конфиденциальности информации – средняя, степень возможного ущерба от нарушения целостности информации – низкая, степень возможного ущерба от нарушения доступности информации – высокая. Какой уровень значимости и класс защищённости Вы присвоите данной ГИС? На основании какого нормативного документа?***

**Ответ:** В соответствии Приказом ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – Требования) Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба.

Воспользовавшись таблицей, приведенной в Приложении №1 Требований, можем определить класс защищенности.

Исходя из вышеизложенного и поставленного вопроса, данной государственной информационной системе необходимо присвоить уровень значимости – **УЗ 1** и класс защищенности – **К1**.

 ***10. Вопрос: Ваша организация эксплуатирует ГИС 3 класса защищённости. Надо или нет применять сертифицированные средства защиты информации? На основании каких нормативных документов?***

**Ответ:** В соответствии пунктом 11 Приказа ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – Требования), для обеспечения защиты информации, содержащейся в Государственной Информационной Системе (далее – ГИС), применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со [статьей 5](http://login.consultant.ru/link/?req=doc;base=RZR;n=221339;fld=134;dst=180) Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании». При этом функции безопасности таких средств должны обеспечивать выполнение Требований.

Организационные меры и средства защиты информации, применяемые в ГИС 3 класса защищенности, должны обеспечивать защиту от угроз безопасности информации, связанных с действиями нарушителей с потенциалом не ниже базового [пункт 25 Требований].

Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. При этом в ГИС 3 класса защищенности применяются средства защиты информации **6 класса**, а также средства вычислительной техники не ниже **5 класса** [пункт 26 Требований].

**Практическое задание №4.**
 ***3. Вопрос: В Вашей организации используются сертифицированное средство защиты информации от несанкционированного доступа Microsoft Windows 7 Service Pack 1. Можно ли его применять в государственных информационных системах 2 класса защищённости? Аргументируйте ответ.***

**Ответ:** Нельзя. В связи с тем, что для государственной информационной системы 2 Класса защищенности применяются средства защиты информации, прошедшие проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей. Для Microsoft Windows 7 Service Pack 1 отсутствует сертификат, подтверждающий данную проверку.

 ***5. Вопрос: В Вашей организации необходимо применять сертифицированные средства межсетевого экранирования. На основании какого документа выбираются межсетевые экраны? Сколько типов, классов защиты межсетевых экранов определено? Чем они различаются?***

**Ответ:** На основании Информационное сообщение ФСТЭК России от 28.04.2016 № 240/24/1986 «Об утверждении требований к межсетевым экранам» (далее – Требование).

В Требованиях выделены следующие типы межсетевых экранов:

* межсетевой экран уровня сети (тип «А»), применяемый на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы. Межсетевые экраны типа «А» могут иметь только программно-техническое исполнение;
* межсетевой экран уровня логических границ сети (тип «Б») – межсетевой экран, применяемый на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы. Межсетевые экраны типа «Б» могут иметь программное или программно-техническое исполнение;
* межсетевой экран уровня узла (тип «В»), применяемый на узле (хосте) информационной системы. Межсетевые экраны типа «В» могут иметь только программное исполнение и устанавливаются на мобильных или стационарных технических средствах конкретного узла информационной системы;
* межсетевой экран уровня веб-сервера (тип «Г»), применяемый на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера). Межсетевые экраны типа «Г» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера;
* межсетевой экран уровня промышленной сети (тип «Д»), применяемый в автоматизированной системе управления технологическими или производственными процессами. Межсетевые экраны типа «Д» могут иметь программное или программно-техническое исполнение и должны обеспечивать контроль и фильтрацию промышленных протоколов передачи данных (Modbus, Profibus, CAN, HART, IndustrialEthernet и (или) иные протоколы).

Для дифференциации требований к функциям безопасности межсетевых экранов выделяются шесть классов защиты межсетевых экранов. Самый низкий класс – шестой, самый высокий – первый.

Межсетевые экраны, соответствующие 6 классу защиты, применяются в государственных информационных системах 3 и 4 классов защищенности, в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровней защищенности персональных данных.

Межсетевые экраны, соответствующие 5 классу защиты, применяются в государственных информационных системах 2 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных.

Межсетевые экраны, соответствующие 4 классу защиты, применяются в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования 2 класса.

Межсетевые экраны, соответствующие 3, 2 и 1 классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

**Практическое задание №5.**

***1. Вопрос: Укажите общий перечень работ, проводимых специалистом по защите информации в ходе эксплуатации аттестованной информационной системы.***

**Ответ:**Согласно пункту 18 Приказа ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает:

* управление (администрирование) системой защиты информации информационной системы;
* выявление инцидентов и реагирование на них;
* управление конфигурацией аттестованной информационной системы и ее системы защиты информации;
* контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

Комментарий преподавателя: Ответ частично не верный. Читайте действующую редакцию приказа ФСТЭК России № 17

**Практическое задание №6.**

***1. Вопрос: Приведите названия документов, содержащих требования о необходимости применения сертифицированных средств защиты информации?***

**Ответ:**

1. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) в редакции от 30.08.2002. пункт 2.16: Для защиты конфиденциальной информации используются сертифицированные по требованиям безопасности информации технические средства защиты информации.
2. Федеральный закон от 27.07.2006 № 152*-*ФЗ «О персональных данных», статья 19, пункт 3: Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.
3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», статья 14 пункт 8: Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.
4. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах пункт 11: Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании» (Собрание законодательства Российской Федерации, 2002, N 52, ст. 5140; 2007, N 19, ст. 2293; N 49, ст. 6070; 2008, N 30, ст. 3616; 2009, N 29, ст. 3626; N 48, ст. 5711; 2010, N 1, ст. 6; 2011, N 30, ст. 4603; N 49, ст. 7025; N 50, ст. 7351; 2012, N 31, ст. 4322; 2012, N 50, ст. 6959).
5. Указ Президента РФ от 17.03.2008 № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» пункт 1: При необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, указанных в подпункте "а" настоящего пункта, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.

 ***2.Вопрос: Чему равен срок действия сертификата соответствия на средство защиты информации? Укажите пункты документов, в которых об этом сказано.***

**Ответ:** В соответствии с пунктом 3.4.1 Приказа ФСБ России от 13.11.1999 № 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия», срок действия сертификата соответствия пять (5) лет.

Согласно пункту 14 Приказа ФСТЭК от 03.04.2018 № 55 "Об утверждении Положения о системе сертификации средств защиты информации", срок действия сертификата соответствия не может превышать 5 лет. Но не более чем указано в заявке на сертификацию.

В соответствии с пунктом 8 постановлением Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации» и Положением о сертификации средств защиты информации по требованиям безопасности информации, утвержденным приказом Гостехкомиссии России от 27.10.1995 № 199, на отдельные экземпляры средств защиты информации, эксплуатируемые на объекте информатизации, продление сроков действия сертификатов соответствия может быть обеспечено организацией, эксплуатирующей данные средства защиты, и проведено по упрощенной схеме.

 ***3.Вопрос: Можно ли использовать в государственной информационной системе
3 класса защищённости средства защиты информации, сроки действия сертификатов соответствия на которые истекли? В каком документе об этом сказано?***

**Ответ:** С 01.08.2018 вступило в силу новое Положение о системе сертификации средств защиты информации, утвержденное приказом ФСТЭК России от 03.04.2018 за № 55. В пункте 15 сказано: «По окончании срока действия сертификата соответствия заявитель вправе подать заявку на продление срока действия сертификата соответствия. Средство защиты информации может применяться по окончании срока действия сертификата соответствия при условии соблюдения требований по безопасности информации и осуществления заявителем его технической поддержки или ФСТЭК явно не отзовет сертификат.

Для определения того что Средство Защиты Информации (далее – СЗИ) соответствует требованиям по безопасности информации и осуществляется его техническая поддержка пользователь СЗИ должен регулярно запрашивать заявителя на сертификацию СЗИ о планах на продолжение/прекращение техподдержки. И обязательно – постоянно отслеживать информационные материалы на сайте ФСТЭК России.

 ***4. Вопрос: К какому типу операционных систем относится программное обеспечение, установленное в банкоматах?***

**Ответ:** В соответствии с приказом ФСТЭК России от 19.08.2016 № 119 «Требования безопасности информации к операционным системам» относится к встраиваемым операционная система **(тип «Б»)**.