Практическая работа 6

Определение требований к системе защиты информации

Теоретическая часть

Требования к защите информации – это установленные правила или нормы, которые должна быть выполнены при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

Формирование требований к защите информации, содержащейся в информационной системе, осуществляется обладателем информации (заказчиком).

Формирование требований к защите информации, содержащейся в информационной системе, осуществляется с учетом ГОСТ Р 51583 "Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения" (далее - ГОСТ Р 51583) и ГОСТ Р 51624 "Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования" (далее - ГОСТ Р 51624) 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.

Требования к системе защиты информации информационной системы определяются в зависимости от класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации.

Требования к системе защиты информации информационной системы включаются в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

* цель и задачи обеспечения защиты информации в информационной системе;
* класс защищенности информационной системы;
* перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;
* перечень объектов защиты информационной системы;
* требования к мерам и средствам защиты информации, применяемым в информационной системе;
* стадии (этапы работ) создания системы защиты информационной системы;
* требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;
* функции заказчика и оператора по обеспечению защиты информации в информационной системе;
* требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуре);
* требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

При определении требований к системе защиты информации информационной системы учитываются положения политик обеспечения информационной безопасности обладателя информации (заказчика), а также политик обеспечения информационной безопасности оператора и уполномоченного лица в части, не противоречащей политикам обладателя информации (заказчика).

В случае создания информационной системы, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, дополнительно определяются требования по защите информации, подлежащие реализации в информационно-телекоммуникационной инфраструктуре центра обработки данных.

Пример

Целью применения мер обеспечения безопасности информации является уменьшение риска либо за счет уменьшения вероятности осуществления угрозы, либо за счет уменьшения эффекта воздействия угрозы.

С экономической точки зрения мера защиты оправдана, если ее эффективность, выраженная через уменьшение ожидаемого экономического ущерба, превышает затраты на ее реализацию.

Рассмотрим концептуальную модель безопасности информации:



Опираясь на виды угроз нашего объекта и на представленную модель можно сформулировать основное требование к защите информации: обеспечить сохранность, целостность, достоверность информации и исключить любую попытку несанкционированного доступа (с применением правового, организационного и инженерно-физического направлений защиты) с использованием всех способов защиты.

Итак, должны быть обеспечены требования:

1) Необходимо иметь явную и четкую методику обеспечения безопасности;

2) Обеспечение идентификации пользователей, имеющих доступ к информации;

3) Информация должна храниться отдельно и защищаться так, чтобы была возможность отслеживать действия, влияющие на безопасность;

4) Средства защиты информации должны включать механизмы контроля доступа ко всем видам информационных и программных ресурсов, которые в соответствии с принципом обоснованности доступа следует разделять между пользователями;

5) Потоки информации должны разграничиваться в зависимости от уровня ее конфиденциальности;

6) Должна быть предусмотрена очистка ресурсов, содержащих конфиденциальную информацию, до перераспределения этих ресурсов другим пользователям;

7) Предупреждение возможных неблагоприятных последствий нарушения порядка доступа к информации;

8) Проведение мероприятий, направленных на предотвращение неправомерных действий в отношении информации;

9) Своевременное обнаружение фактов неправомерных действий в отношении информации;

10) Недопущение воздействия на технические средства информационной системы общего пользования, в результате которого может быть нарушено их функционирование;

11) Возможность оперативного восстановления информации, модифицированной или уничтоженной вследствие неправомерных действий;

12) Проведение мероприятий по постоянному контролю за обеспечением защищенности;

13) Возможность записи и хранения сетевого трафика;

14) Система защиты информации должна точно выполнять свои функции в соответствии с основными принципами и быть изолированной от пользователей.

Практическая часть

Для своего варианта определить требования к системе защиты информации.