Лабораторная работа. Защита государственных информационных систем (ГИС), обрабатывающих ПДн.

Цель лабораторной работы:

познакомиться с аспектами защиты ГИС.

Задачи лабораторной работы:

разработать приложение, автоматизирующее процесс определения класса защищённости ГИС. При этом степень возможного ущерба должна определяться экспертами с помощью метода Дельфи. Эксперт оценивает значимость негативных последствий от нарушения конфиденциальности, целостности и доступности по шкале от 0 до 100. Экспертные оценки должны генерироваться в программе автоматически. Количество экспертов задаётся пользователями. В программе на каждом раунде метода Дельфи оценка одного и того же эксперта не может разниться более чем на 15%. Количество раундов задаётся пользователем. Значения от 0 до 20 будут обозначать незначительные негативные последствия; от 21 до 70 – умеренные негативные последствия; 71-100 – значительные негативные последствия. Масштаб информационной системы определяется пользователем.

Теория:

в Российской Федерации существует несколько сотен государственных информационных систем. Большинство государственных информационных систем обрабатывает персональные данные. Например, просмотреть реестр федеральных государственных информационных систем можно по следующей ссылке: http://rkn.gov.ru/it/register/

В соответствии с Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» государственные информационные системы (ГИС) создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

При этом к ГИС относятся федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов, а также муниципальные информационные системы, созданные на основании решения органа местного самоуправления.

С 01 сентября 2013 года требования о защите информации, содержащейся в ГИС, определяются Приказом ФСТЭК России от 11.02.2013г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Данный Приказ определил 4 класса защищенности ГИС, устанавливаемых в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы: первый класс (К1), второй класс (К2), третий класс (К3), четвертый класс (К4). Самый низкий класс – четвертый, самый высокий – первый.

Класс защищенности информационной системы определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности, целостности или доступности информации:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

- высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;
- средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

• низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Для определения степени возможного ущерба от нарушения конфиденциальности, целостности или доступности могут применяться национальные стандарты и (или) методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

Масштаб информационной системы определяется назначением и распределенностью сегментов информационной системы.

Информационная система имеет федеральный масштаб, если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.

Информационная система имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

Информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

При обработке персональных данных в информационной системе определение класса защищенности информационной системы осуществляется с учетом требуемого уровня защищенности персональных данных, установленного в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119. При этом в соответствии с пунктом 27 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17, должно быть обеспечено соответствующее соотношение

класса защищенности государственной информационной системы с уровнем защищенности персональных данных. В случае, если определенный в установленном порядке уровень защищенности персональных данных выше чем установленный класс защищенности государственной информационной системы, то **осуществляется повышение класса защищенности** до значения, обеспечивающего выполнение пункта 27 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3
УЗ 4	К3	К3	К4

Для обеспечения защиты информации, содержащейся в ГИС, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в информационной системе;
- разработка системы защиты информации информационной системы;
- внедрение системы защиты информации информационной системы;
- аттестация информационной системы по требованиям защиты информации и ввод ее в действие;
- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;
- обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Приказ ФСТЭК России от 11.02.2013г. №17 определил перечень мер защиты и их базовые наборы, которые должны быть реализованы в зависимости от класса защищенности ГИС, а также установил требование об обязательной сертификации применяемых средств защиты информации.

Метод Дельфи.

Основной принцип метода Дельфи: если опросить людей, обладающих компетенцией в интересующем нас вопросе, их усреднённая оценка обычно будет точна более чем на 80%. Если провести второй раунд, предварительно ознакомив экспертами с результатами первого, то результативность становится ещё выше. Модификация метода: брать среднюю оценку после отбрасывания крайних значений. Данный метод рекомендуется применять, если эксперты не могут подкрепить своё мнение серьёзными аргументами. Экспертов должно быть не менее трёх, а лучше пять.

Эксперты	Раунд 1	Раунд 2
Эксперт 1	50	55
Эксперт 2	65	60
Эксперт 3	100	80
Эксперт 4	30	50
Эксперт 5	60	60
Итого	**58**	**58**

Рекомендуемая литература:

1) http://www.securitycode.ru/solutions/zashchita-gosudarstvennykh-informatsionnykh-sistem/
2) http://www.securitylab.ru/blog/personal/Business_without_danger/38311.php
3) https://kontur.ru/articles/1609
4) http://www.altx-soft.ru/files/groups/405.pdf
5) http://www.inventech.ru/pub/methods/metod-0013/