МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Новоуральский технологический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»
(НТИ НИЯУ МИФИ)
Колледж НТИ

Цикловая методическая комиссия информационных технологий

ОТЧЕТ №4
ПО ПРАКТИЧЕСКОМУ ЗАНЯТИЮ НА ТЕМУ

«Анализ источников, каналов распространения и каналов утечки информации»

МП.05 «Разработка программного обеспечения компьютерных сетей»
МДК.05.01 «Защита информации в КС»

Специальность СПО 09.02.03
«Программирование в компьютерных системах»

очная форма обучения
на базе основного общего образования

Выполнил
студент группы КПР–47 Д
Егорушкин И.А. 11.11.2020 _____
дата подпись

Проверил
преподаватель _____ _____
Горницкая И.И. дата подпись

Новоуральск 2020

Цель работы: формирование навыка работы с нормативными документами по исследуемому вопросу; анализ угроз информационной безопасности

Оборудование:

ПК – процессор AMD Ryzen 7 2700X ОЗУ 32 Гб

Программное обеспечение:

Операционная система MS Windows 10 Professional MS Word

Сайт nsti

Виды возможных угроз

физической целостности	+
логической целостности	+
содержания	+
конфиденциальности	+
прав собственности на информацию	+

Характер происхождения угроз

Умышленные факторы	
хищение носителей информации;	+
подключение к каналам связи;	+
перехват электромагнитных излучений (ЭМИ);	-
несанкционированный доступ;	+
разглашение информации;	+
копирование данных.	+
Естественные факторы	
несчастные случаи (пожары, аварии, взрывы);	+

стихийные бедствия (ураганы, наводнения, землетрясения);	+
ошибки в процессе обработки информации (ошибки пользователя, оператора, сбои аппаратуры)	+

Классы каналов несанкционированного получения информации

1) Подслушивание разговоров (в том числе аудиозапись).	-
2) Установка закладных устройств в помещение и съем информации с их помощью.	-
3) Выведывание информации обслуживающего персонала на объекте.	+
4) Фотографирование или видеосъемка носителей информации внутри помещения.	-
5) Ввод программных продуктов, позволяющих злоумышленнику получать информацию.	-
6) Копирование информации с технических устройств отображения (фотографирование с мониторов и др.).	+
7) Получение информации по акустическим каналам (в системах вентиляции, теплоснабжения, а также с помощью направленных микрофонов).	-
8) Получение информации по виброакустическим каналам (с использованием акустических датчиков, лазерных устройств).	-
9) Подключения к линиям связи.	+

Источники появления угроз

1) Люди которые участвуют в переговорах	-
2) технические устройства	+
3) Третьи лица заинтересованные в получении информации тайных конфиденциальных переговоров	-

Причины нарушения целостности информации

угрозы нарушения физической и логической целостности, а также содержания информации (несанкционированная модификация). Их можно объединить в причины нарушения целостности информации (ПНЦИ);

Потенциально возможные злоумышленные действия

Потенциально возможные злоумышленные действия

Кража конфиденциальных данных

Нарушение работоспособности сервиса

Определить класс защищенности автоматизированной системы.

Класс А1

1. Что такое информационный риск?

Информационный риск — это, с одной стороны, вероятность порчи информации как специфического объекта и, с другой стороны, вред, который причиняется специфическими средствами (информацией).

2. Какие существуют методики оценки рисков и управления ими?

В системе управления риском важнейшей составляющей является оценка риска. Степень риска можно определить количественным или качественным способом. При качественном анализе выявляют не только виды риска, но определяют и возможные причины, влияющие на уровень риска. Внешне описательная методика качественной оценки подводит к количественному результату – оценки стоимости предполагаемых последствий в случае реализации факторов риска

3. Какие формулы используются при количественной оценке информационных рисков?

Количественный метод. Количественная оценка рисков применяется в ситуациях, когда исследуемые угрозы и связанные с ними риски можно сопоставить с конечными

количественными значениями, выраженными в деньгах, процентах, времени, человекоресурсах и проч. Метод позволяет получить конкретные значения объектов оценки риска при реализации угроз информационной безопасности. При количественном подходе всем элементам оценки рисков присваивают конкретные и реальные количественные значения.

Как провести количественную оценку рисков?

1. Определить ценность информационных активов в денежном выражении.

2. Оценить в количественном выражении потенциальный ущерб от реализации каждой угрозы в отношении каждого информационного актива.

Следует получить ответы на вопросы «Какую часть от стоимости актива составит ущерб от реализации каждой угрозы?», «Какова стоимость ущерба в денежном выражении от единичного инцидента при реализации данной угрозы к данному активу?».

3. Определить вероятность реализации каждой из угроз ИБ.

Для этого можно использовать статистические данные, опросы сотрудников и заинтересованных лиц. В процессе определения вероятности рассчитать частоту возникновения инцидентов, связанных с реализацией рассматриваемой угрозы ИБ за контрольный период (например, за один год).

4. Определить общий потенциальный ущерб от каждой угрозы в отношении каждого актива за контрольный период (за один год).

Значение рассчитывается путем умножения разового ущерба от реализации угрозы на частоту реализации угрозы.

5. Провести анализ полученных данных по ущербу для каждой угрозы.

По каждой угрозе необходимо принять решение: принять риск, снизить риск либо перенести риск.

Качественный метод

К сожалению, не всегда удается получить конкретное выражение объекта оценки из-за большой неопределенности. Как точно оценить ущерб репутации компании при появлении информации о произошедшем у нее инциденте ИБ? В таком случае применяется качественный метод.

При качественном подходе не используются количественные или денежные выражения для объекта оценки. Вместо этого объекту оценки присваивается показатель, про ранжированный по трехбалльной (низкий, средний, высокий), пятибалльной или десятибалльной шкале (0… 10). Для сбора данных при качественной оценке рисков применяются опросы целевых групп, интервьюирование, анкетирование, личные встречи.

Анализ рисков информационной безопасности качественным методом должен проводиться с привлечением сотрудников, имеющих опыт и компетенции в той области, в которой рассматриваются угрозы.

Вывод: входе работе было произведённое исследование сайта nsti на анализ угроз информационной безопасности