**Практическая работа №20. Оценка уязвимости информации**

**Цель работы:** Ознакомиться с алгоритмами оценки уязвимости информационной безопасности.

**Практическое задание**

ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.»

**Приложение С. Перечень типичных видов угроз.**

**Приложение D.** **Примеры общих уязвимостей.**

**Приложение E. Типология методов анализа риска**

База сотрудников, хранящаяся на сервере –она нужна для издательства, так как на ней хранится информация о всех сотрудниках издательства.

Хранилище на электронном носителе- содержит всю информацию нужную для издательства. Информация доступна только определённым лицам и не должна попасть в руки злоумышленников

Бухгалтерская документация – информация затраты издательства, зарплата сотрудникам

**Оценка ценности информационных активов**

В этом издательстве мы выделили 3 важных актива и поставим ему оценку от 0 до 4.

База сотрудников информация о сотрудниках. Оценка этого актива 2.

**Возможный ущерб:**

нарушение законов и/или подзаконных актов.

1. Хранилище на электронном носителе оценивается тем что находится в нём. Оценка этого актива 3. Возможный ущерб: потеря престижа/негативное воздействие на репутацию
2. Бухгалтерская документация самые цены сведенья. Оценка этого актива 4. Возможный ущерб: финансовые потери, нарушение конфиденциальности коммерческой информации, снижение эффективности бизнеса.

**Контрольные вопросы**

1. Уязвимости системы защиты информации

Размещение в зонах возможного затопления (возможна, например, угроза затопления).

Отсутствие механизмов идентификации и аутентификации, например, аутентификации пользователей (возможна, например, угроза нелегального проникновения злоумышленников под видом законных пользователей)

Отсутствие необходимых знаний по вопросам безопасности (возможна, например, угроза ошибок пользователей).

1. Угрозы ИБ

Затопление. Размещение в зонах возможного затопления

В зависимости от того на сколько затоплено помещение, можно сказать высока ли угроза потери важнейшей информации. При затопленности, общего помещения, например, из-за наводнения, потери будут колоссальны. Вся информация будет уничтожена.

Угроза нелегального проникновения злоумышленников под видом законных пользователей. Могут быть выкрадены очень важные документы для организации. И приведет к упадку Издательства.

Угроза ошибок пользователей. Не значительна ошибка. Вызванная сотрудником Издательства.

1. Оценка рисков

База сотрудников:

При угрозе затопление вероятность возникновения угрозы мала, а легкость возникновения угрозы в уязвимых местах имеет высокое значение, то частота будет равна 2.

При угрозе нелегального проникновения злоумышленников под видом законных пользователей вероятность возникновения угрозы высока, а легкость возникновения угрозы в уязвимых местах имеет среднее значение, то частота будет равна 3.

При угрозе ошибок пользователей вероятность возникновения угрозы высока, а легкость возникновения угрозы в уязвимых местах имеет высокое значение, то частота будет равна 4.

Хранилище на электронном носителе:

При угрозе затопление вероятность возникновения угрозы мала, а легкость возникновения угрозы в уязвимых местах имеет высокое значение, то частота будет равна 2.

При угрозе нелегального проникновения злоумышленников под видом законных пользователей вероятность возникновения угрозы высока, а легкость возникновения угрозы в уязвимых местах имеет среднее значение, то частота будет равна 3.

При угрозе ошибок пользователей вероятность возникновения угрозы высока, а легкость возникновения угрозы в уязвимых местах имеет высокое значение, то частота будет равна 4.

Бухгалтерская документация:

При угрозе затопление вероятность возникновения угрозы мала, а легкость возникновения угрозы в уязвимых местах имеет высокое значение, то частота будет равна 2.

При угрозе нелегального проникновения злоумышленников под видом законных пользователей вероятность возникновения угрозы высока, а легкость возникновения угрозы в уязвимых местах имеет среднее значение, то частота будет равна 3.

При угрозе ошибок пользователей вероятность возникновения угрозы высока, а легкость возникновения угрозы в уязвимых местах имеет высокое значение, то частота будет равна 4.

