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 №7
ПО ПРАКТИЧЕСКОМУ ЗАНЯТИЮ НА ТЕМУ

«АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

ПМ.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. 11.12.2020 _____
дата подпись

Проверил
преподаватель _____ _____
Горницкая И.И. дата подпись

Новоуральск 2020

Цель работы: Анализ рисков информационной безопасности

Оборудование:

AMD Ryzen 5 3550U

ОЗУ 8 Гб

Программное обеспечение:

Windows 10 Professional 64 бит;

Ход работы:

Задание

Номер варианта	Организация	Метод оценки риска (см. Приложение Е ГОСТа)
2	Поликлиника	2

Обоснование выбора информационных активов организации

- База сотрудников, хранящаяся на сервере –она нужна для поликлиники , так как на ней хранится информация о всех сотрудниках.
- Электронная мед карта, хранит всю информацию о заболевании, и историю пациентов на сервере.
- Запись приёмов, хранит всю историю приёмов , а также назначенные приёмы на сервере

Оценка ценности информационных активов

База сотрудников информация о сотрудниках. Оценка этого актива 2.
Возможный ущерб: нарушение законов и/или подзаконных актов.

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

Уязвимости системы защиты информации

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).

Угроз ИБ

1. Угроза нелегального проникновения злоумышленников под видом законных пользователей. Могут быть выкрадены очень важные документы для организации. И приведет к упадку Издательства.
2. Угроза ошибок пользователей. Не значительна ошибка, вызванная сотрудником.
3. Физическое повреждение оборудования или выхода из строя.

Оценка рисков

БД сотрудники:

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.

При физическом повреждении оборудования вероятность возникновения угрозы средняя, а легкость возникновения угрозы в уязвимых местах имеет среднее значение, то частота будет равна 2.

Электронная мед карта:

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 средняя, а легкость возникновения угрозы в уязвимых местах имеет высокое значение, то частота будет равна 4.

При физическом повреждении оборудования вероятность возникновения угрозы средняя, а легкость возникновения угрозы в уязвимых местах имеет среднее значение, то частота будет равна 2.

Запись приёмов:

При угрозе нелегального проникновения злоумышленников под видом законных пользователей вероятность возникновения угрозы минимальная, а легкость возникновения угрозы в уязвимых местах имеет среднее значение, то частота будет равна 2.

При угрозе ошибок пользователей вероятность возникновения угрозы минимальная, а легкость возникновения угрозы в уязвимых местах имеет средние значение, то частота будет равна 2.

При физическом повреждении оборудования вероятность возникновения угрозы средняя, а легкость возникновения угрозы в уязвимых местах имеет среднее значение, то частота будет равна 2.

Дескриптор угроза	Оценка воздействия (ценности актива) b	Вероятность возник- новения угрозы c	Мера риска d	Ранг угрозы e
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Вывод: в результате проведенного исследования были рассмотрены и выявлены угрозы ИБ в сфере обороны, объекты, информационную безопасность которых необходимо обеспечивать, их уязвимости. Была проведен анализ отношений между угрозами, уязвимостями, объектами, реализациями угроз и их источниками.