

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 №8

ПО ПРАКТИЧЕСКОМУ ЗАНЯТИЮ НА ТЕМУ

**«ПОСТРОЕНИЕ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРЕДПРИЯТИЯ»**

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

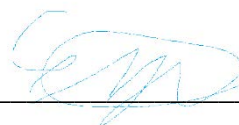
Выполнил

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 |

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

Настоящий документ представляет собой концепцию обеспечения информационной безопасности предприятия:

- Основные принципы формирования перечня критичных ресурсов, нуждающихся в защите, формируемого в процессе проведения аудита безопасности и анализа рисков. Данный перечень должен включать в себя описание физических, программных и информационных ресурсов с определением стоимости ресурсов и степени их критичности для предприятия.
- Основные принципы защиты, определяющие стратегию обеспечения информационной безопасности (ИБ) и перечень правил, которыми необходимо руководствоваться при построении системы обеспечения информационной безопасности (СОИБ) предприятия.
- Модель нарушителя безопасности, определяемую на основе обследования ресурсов системы и способов их использования.
- Модель угроз безопасности и оценку рисков, связанных с их осуществлением, формируемую на основе перечня критичных ресурсов и модели нарушителя, которая включает определение вероятностей угроз и способов их осуществления, а также оценку возможного ущерба.
- Требования безопасности, определяемые по результатам анализа рисков.
- Меры обеспечения безопасности организационного и программно-технического уровня, предпринимаемые для реализации перечисленных требований.
- Ответственность сотрудников предприятия за соблюдение установленных требований ИБ при эксплуатации информационной системы (ИС) предприятия.

Концепции по обеспечению информационной безопасности

1.2. Цели системы информационной безопасности

Конечной целью создания системы обеспечения безопасности информационных технологий является предотвращение или минимизация ущерба (прямого или косвенного, материального, морального или иного), наносимого субъектам информационных

отношений посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

1.3. Задачи системы информационной безопасности.

Задачи системы информационной безопасности является невозможность нанесения вреда безопасности поликлиники, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз). Основными задачами системы ИБ поликлиники являются: своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба его интересам;

2. Проблемная ситуация в сфере информационной безопасности

Цифровизация в сфере здравоохранения повышает эффективность оказания медицинских услуг. Электронный документооборот в медучреждениях облегчает ведение учета, выводит качество обработки и хранения данных на новый уровень, повышает эффективность контроля за оказанными медицинскими услугами, распределением финансовых ресурсов и т. д. Но такая цифровизация имеет и обратную сторону — повышаются риски нарушения информационной безопасности, когда информация из электронных баз данных больниц и клиник используют в корыстных целях. В сфере здравоохранения эти риски особенно велики.

2.1. Объекты информационной безопасности.

К объектам информационной безопасности относятся:

- 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

2.2. Определение вероятного нарушителя.

Данному предприятию могут представлять угрозу следующие типы нарушителей:

- Нарушитель, который получает несанкционированный доступ.
- Сотрудник предприятия , который может нанести ущерб из-за неправильных действий.
- Пациентов и их медицинские данные

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

Классификации угроз:

- Потеря данных

Отсутствие резервных или повреждение резервных копий, при отказе основной системы.

- Утечки информации

Взлом зашифрованных каналов связи, получение пассивного доступа к базам данных.

- Несанкционированный доступ

Может произойти вследствие взлома каналов связи.

- Мошенничество

Угроза копирования сервиса и создания фишинговой копии, которая снизит поток клиентов, а также, которая способна значительно подмочить репутацию предприятия.

Основные непреднамеренные искусственные угрозы:

- Пожар

Зависит от того, где будет располагаться предприятие и насколько на нём будет соблюдаться техника пожарной безопасности.

- Затопление

Зависит от состояния сантехнических узлов непосредственно на предприятии, а также его соседей.

- Время (износ материалов)

Износ жёстких дисков, SSD, выход из строя процессоров и т.д.

Основные преднамеренные искусственные угрозы:

- Халатность сотрудников (главная угроза ИБ)
- Кража информации (возможно проведение сотрудниками предприятия или злоумышленниками)
- Кража оборудования (возможно проведение сотрудниками предприятия)
- Финансовое мошенничество
- Саботаж (возможно проведение сотрудниками предприятия)
- Хакерские атаки
- Вредоносные программы (если не соблюдается политика безопасности предприятия)

2.4. Основные виды угроз информационной безопасности Предприятия.

| Дескриптор угроз а | Оценка воздействия (ценности актива) b | Вероятность возникновения угрозы с | Мера риска a d | Ранг угрозы e |
|--------------------|--|------------------------------------|----------------|---------------|
| Угроза А | 5 | 2 | 10 | 2 |
| Угроза В | 2 | 4 | 8 | 3 |
| Угроза С | 3 | 5 | 15 | 1 |
| Угроза D | 1 | 3 | 3 | 5 |
| Угроза E | 4 | 1 | 4 | 4 |
| Угроза F | 2 | 4 | 8 | 3 |

3. Механизмы обеспечения информационной безопасности Предприятия

Обеспечение безопасности медицинской информации законодательно регламентировано на федеральном уровне. Для защиты сведений применяют следующие методы:

- Организационно управленческие (обозначение рамок и условий работы ресурсов, регламентация системы взаимодействия между пользователями и администратором сети);
- правовые (ответственность за нарушение правил);
- технические (программное и аппаратное обеспечение, которое защищает от несанкционированного доступа и обеспечивает авторизацию пользователей).

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

Использование ОС

- Astra Linux
- Эльбрус на процессоре Эльбрус
- GosLinux

3.2. Основные направления политики в сфере информационной безопасности.

Основные направления политики в сфере информационной безопасности являются:

Создать отдельные системы одна с выходом в интернет другая внутренняя с прокси сервером.

3.3. Планирование мероприятий по обеспечению информационной безопасности

Предприятия.

- Определения общих правил обработки информации
- Определение должностных обязанностей и степени ответственности сотрудников

3.4. Критерии и показатели информационной безопасности Предприятия.

Безопасность предприятия определяют следующие показатели:

- конфиденциальность
- целостность
- доступность

После определения данных показателей, мы можем оценить общее состояние системы безопасности.

4. Мероприятия по реализации мер информационной безопасности

Предприятия

4.1. Организационное обеспечение информационной безопасности.

Задачи организационного обеспечения безопасности:

- ограничение доступа на объект и к ресурсам
- разграничение доступа к ресурсам
- планирование мероприятий(возможно развлекательного содержания, к примеру вечеринки, тимбилдинги и т.д.)
- разработка документации
- воспитание и обучение обслуживающего персонала и пользователей (для персонала - проведение регулярных обучающих курсов и тестирований, для пользователей - грамотная рекламная осведомительная компания).

Подразделения, занятые в обеспечении безопасности:

- Руководство организации
- Подразделение обеспечения информационной безопасности

- Пользователи и обслуживающий персонал

Взаимодействие подразделений, занятых информационной безопасностью:

- Руководство организации определяет правила и согласовывает методы обеспечения информационной безопасности
- Подразделение обеспечения информационной безопасности занимается разработкой и реализацией систем защиты информации
- Пользователи и обслуживающий персонал соблюдает правила, установленные руководством

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.

Техническое обеспечение информационной безопасности предприятия предусматривает:

- Надежное инженерно-техническое перекрытие вероятных путей несанкционированного вторжения в охраняемые пределы
 - Высокую техническое обеспечение основных и резервных сил охраны к оперативному противодействию преступным действиям
 - Эффективные системы пожаротушения
 - Влагоустойчивые корпуса оборудования
-
- Защита информационных ресурсов от несанкционированного доступа.
 - Антивирусное ПО на компьютерах сотрудников
 - Сейфы для документов
 - Звуконепроницаемые комнаты для аудиенций со шторами (или отсутствием окон)
 - Персональные ключи для каждого кабинета и рабочего места
 - Система разграничения доступа

- Средства комплексной защиты от потенциальных угроз.

Каждая проблема имеет соответствующее решение. В данном случае - комплексное.

Данное решение подразумевает использование разнообразных антивирусных и криптографических средств, а также средств разграничения доступа.

Подобные подходы предусматривают анализ и оптимизацию всей системы, а не отдельных ее частей, что позволяет обеспечить баланс характеристик, тогда как улучшение одних параметров нередко приводит к ухудшению других.

Комплексный подход обязывает к проведению детального анализа интегрируемой системы, оценку угроз безопасности, изучение средств, используемых при построении системы, их возможностей, анализ соотношения внутренних и внешних угроз и оценку возможности внесения изменений в систему.

- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия .

Договор является стержнем юридических отношений с партнерами предприятия.

Грамотная договорная работа является фундаментом, обеспечивающим защиту интересов предприятия при возникновении конфликтных ситуаций. Уже при проведении переговоров и заключении договора целесообразно предусмотреть возможные варианты споров и наметить способы выхода из конфликтных ситуаций.

- Правовое обеспечение применения электронной цифровой подписи. Электронная Цифровая Подпись (ЭЦП) является полным электронным аналогом обычной подписи на бумаге, но реализуется не с помощью графических изображений, а с помощью математических преобразований над содержимым документа. Особенности математического алгоритма создания и проверки ЭЦП гарантируют невозможность подделки такой подписи посторонними лицами, чем достигается неопровержимость авторства.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

Оценка эффективности системы позволяет вносить необходимые для её повышения изменения, а также прогнозировать дальнейшие результаты деятельности внедряемой системы.

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.