Поромошкин Андрей Анатольевич,

студент, МГТУ им. Г.И. Носова,

г. Магнитогорск,

Баранкова Инна Ильинична,

заведующая кафедрой ИиИБ,

профессор, доктор технических наук, аккредитованный эксперт РосОбрНадзора,

член Координационного совета по подготовке кадров

в области информационной безопасности по УРФО Носова,

г. Магнитогорск

РАЗРАБОТКА МОДЕЛИ НАРУШИТЕЛЯ ДЛЯ МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ

Аннотация. В данной статье разрабатывается модель нарушителя для медицинского центра. На основе данной модели формируются предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе, а также потенциал нарушителей и возможных способах реализации угроз безопасности информации.

Ключевые слова: информация, безопасность, персональные данные (ПДн), модель, нарушитель, защита информации, медицинская информационная система (МИС), автоматизированная система (АС).

Защита персональных данных в медицинских учреждениях является одной из главных задач, поэтому нарушение целостности, конфиденциальности и доступности ПДн может привести к угрозе жизни или здоровья человека.

Но также можно выделить такие возможные цели злоумышленника:

- служебная информация;
- персональные данные сотрудников;
- аутентификационная информация;

• информация о структуре, принципах МИС;

Для оценки возможностей нарушителей по реализации угроз необходимо составить предположение о возможных типах, видах и цели (мотивации) нарушителей, которые могут реализовать угрозы безопасности информации.

На основе данной представленной в методическом документе [1] таблице “Виды нарушителя и их возможные цели (мотивация) реализации угроз безопасности информации” составим таблицу для медицинского учреждения.

Таблица 1.

Виды нарушителя и их возможные цели (мотивация) реализации угроз безопасности информации в медицинском учреждении.

№ вида	Виды нарушителя	Типы нарушителя	Возможные цели (причины) реализации угроз безопасности информации
1	Медицинский персонал (врачи и медсестры)	Внутренний	Непреднамеренные, неосторожные действия (халатность). Шантаж с целью финансовой выгоды. Месть за ранее причинённый ущерб.
2	Администратор информационной системы	Внутренний	Причинение имущественного ущерба путем мошенничества или иным путем. Месть за ранее причинённый ущерб. Выявление уязвимостей с целью получения финансовой выгоды. Шантаж с целью финансовой выгоды.

3	Пациенты	Внутренний	Любопытство или желание самореализации. Распространение информации в интернете с целью испортить репутацию. Шантаж с целью финансовой выгоды.
4	Обслуживающий персонал	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные действия (халатность). Шантаж с целью финансовой выгоды. Месть за ранее причинённый ущерб.
5	Внешние субъекты (физические лица)	Внешний	Причинение имущественного ущерба путем мошенничества или иным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Шантаж с целью финансовой выгоды. Распространение информации в интернете с целью испортить репутацию.

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности ин-

формации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования[2].

Медицинский персонал являются пользователями информационной системы. Они имеют непосредственный доступ к персональным данным пациента и поэтому несут самую большую угрозу. Их непреднамеренные и неосторожные действия могут привести к изменению информации о состоянии здоровья, что может привести к угрозе жизни или здоровью пациента.

У администратора информационной системы есть возможность к реализации угрозы связанной с доступом непосредственно к защищаемой информации, обрабатываемой и хранимой в МИС (информации о состоянии здоровья пациентов, диагноз, курс лечения) и обусловлены возможностью нарушения целостности и конфиденциальности информации о состоянии здоровья пациента. Также администратор информационной системы имеет доступ к техническим и программным средствам МИС, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями. Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и МИС в целом, а также с применяемыми принципами и концепциями безопасности. Таким образом, администратор имеет самый высокий потенциал.

Обслуживающий персонал, пациенты и внешние субъекты не имеют непосредственного доступа к защищаемой информации. Обслуживающий персонал имеет возможность получить информацию об уязвимостях МИС путем злоупотребления доверием или халатностью медицинского персонала. Пациенты, путем любопытства, могут воспользоваться информацией с целью шантажа

или распространения информации в интернете. Внешние субъекты с целью шантажа имеют возможность использования акустических, виброакустических каналов утечки информации, хоть данные угрозы и являются неактуальными для медицинского учреждения.

На основе выше описанных данных составим таблицу 2 “Потенциал нарушителей и их возможности”.

Таблица 2.

Потенциал нарушителей и их возможности

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
1	Нарушители с базовым (низким) потенциалом	Внешние субъекты (физические лица), обслуживающий персонал, посетители	Имеют возможность получить информацию об уязвимостях отдельных компонент медицинской информационной системы, путем злоупотребления доверием. Неосторожные и неквалифицированные действия персонала медицинского учреждения. Использование акустических, виброакустических каналов утечки информации и других уязвимостей МИС.
2	Нарушители с базовым повышенным (средним) потенциалом	Медицинский персонал	Возможное нарушение конфиденциальности и целостности информации путем непосредственного доступа к ней.
3	Нарушители с высоким потенциалом	Администратор информационной системы	Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защища-

			емой информации, обрабатываемой и хранимой в МИС, а также к техническим и программным средствам МИС, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями. Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и МИС в целом, а также с применяемыми принципами и концепциями безопасности.

Таким образом, с помощью данной модели нарушителя определяется вид нарушителя с самым высоким потенциалом и его возможность реализации угрозы. Хотя самый высокий потенциал нарушителя у администратора безопасности, типичным нарушителем в медицинском учреждении является медицинский персонал. Для понижения потенциала нарушителя следует регламентировать действия медицинского персонала с возможными серьезными последствиями за нарушение регламента.

СПИСОК ЛИТЕРАТУРЫ

1. Методический документ «Методика определения угроз безопасности информации в информационных системах». разработан и утвержден 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.

2. Михайлова У.В., Фасхеев К.В., Веденеев В.А. Разработка модели угроз и модели нарушителя с целью создания системы технической защиты информации выделенного помещения на базе МГТУ // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 76-ой междунар. науч.-техн. конф. Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2018. – Т. 1. – С. 316-316.