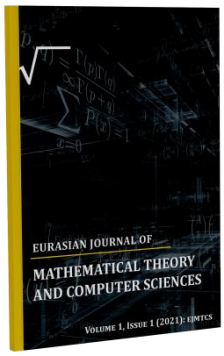
EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.916 www.in-academy.uz



ИСТОЧНИКИ, ВИДЫ И СПОСОБЫ ДЕСТАБИЛИЗИРУЮЩЕГО ВОЗДЕЙСТВИЯ НА ЗАЩИЩАЕМУЮ ИНФОРМАЦИЮ В МЕДИЦИНСКОМ УЧРЕЖДЕНИИ

[1]Гуломов Шерзод Ражабоевич
[2]Маматова Динора Мавлон қизи
[3]Маматов Эратбек Мухивиддинович
ТУИТ имени Мухаммада ал-Хоразмий, +998 99 555 50 03
https://www.doi.org/10.5281/zenodo.7932619

ARTICLE INFO

Received: 03rd May 2023
Accepted: 12th May 2023
Online: 13th May 2023

KEY WORDS

ABSTRACT

В этом статье анализировано источники, виды и способы дестабилизирующего воздействия на защищаемую информацию в медицинском учреждении, которое приводить к нарушению информационную безопасности системы.

Современные медицинские учреждения все больше используют компьютерные системы, информационные базы данных и средства связи для регистрации, хранения, передачи и обработки медицинской информации. Это связано с увеличением объема и сложности данных, а также необходимостью обеспечения доступности информации для медицинских работников и пациентов.

К источникам дестабилизирующего воздействия на информацию относятся:

1.люди;

2.технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи и системы обеспечения их функционирования;

3.природные явления.

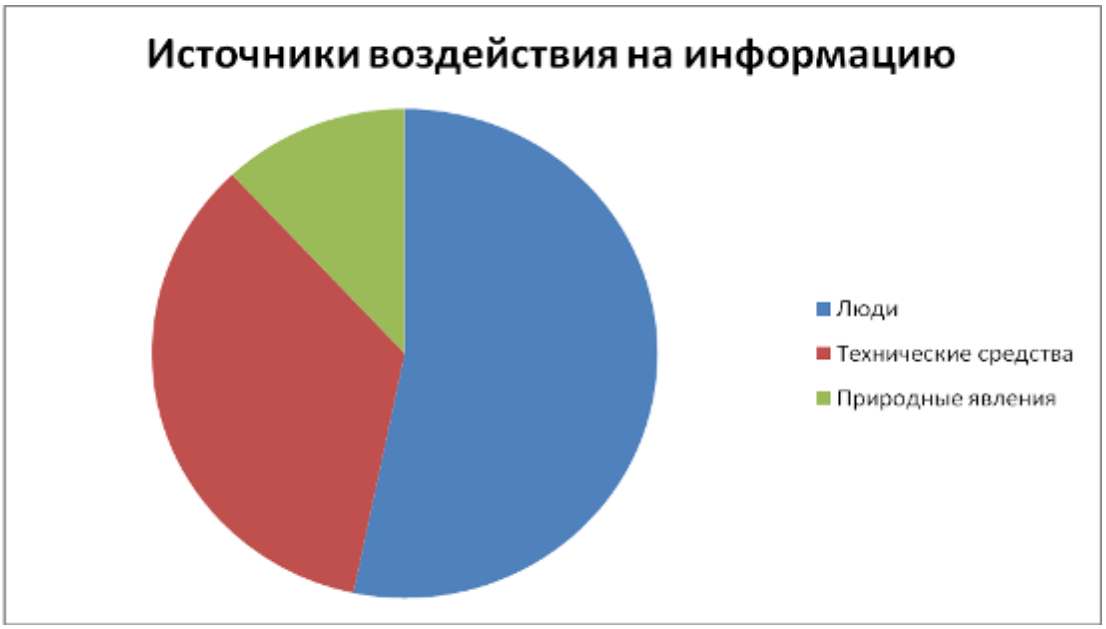


Рисунок 1. Источники дестабилизирующего воздействия на защищаемую информацию

Самым распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию являются люди. К ним относятся:

- сотрудники данного медицинского учреждения;
- лица, не работающие в ЛПУ, но имеющие доступ к защищаемой информации в силу служебного положения (из контролирующих органов государственной и муниципальной власти и др.);
- сотрудники посторонних фирм, оказывающих услуги;
- лиц, для которых защищаемая информация представляет ценность, хакеры.

Эти категории людей подразделяются на две группы:

- имеющие доступ к носителям данной защищаемой информации, техническим средствам ее отображения, хранения, обработки, воспроизведения, передачи и системам обеспечения их функционирования и
- не имеющие такового.

Самым многообразным этот источник является потому, что ему, по сравнению с другими источниками, присуще значительно большее количество видов и способов дестабилизирующего воздействия на информацию [1].

Самым опасным этот источник является потому, что он самый массовый; воздействие с его стороны носит регулярный характер; его воздействие может быть не только непреднамеренным, но и преднамеренным и оказываемое им воздействие может привести ко всем формам проявления уязвимости информации.

Виды и способы дестабилизирующего воздействия на защищаемую информацию дифференцируются по источникам воздействия. Самое большее количество видов и способов дестабилизирующего воздействия имеет отношение к людям**.**

Со стороны людей возможны следующие виды воздействия, приводящие к уничтожению, искажению и блокированию:

1. Непосредственное воздействие на носители защищаемой информации.
2. Несанкционированное распространение конфиденциальной информации.
3. Вывод из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи.
4. Нарушение режима работы перечисленных средств и технологии обработки информации.
5. Вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

Способами непосредственного воздействия на носители защищаемой информации могут быть:

-физическое разрушение носителя (поломка, разрыв и др.);
-создание аварийных ситуаций для носителей (поджог, искусственное затопление, взрыв и т.д.);
-удаление информации с носителей (замазывание, стирание, обесцвечивание и др.);
-создание искусственных магнитных полей для размагничивания носителей;
-внесение фальсифицированной информации в носители;

-непреднамеренное оставление их в неохраняемой зоне, чаще всего в общественном транспорте, магазине, на рынке, что приводит к потере носителей.

Несанкционированное распространение конфиденциальной информации может осуществляться путем:

- словесной передачи (сообщения) информации;
- передачи копий (снимков) носителей информации;
- показа носителей информации;
- ввода информации в вычислительные сети;
- опубликования информации в открытой печати;
- использования информации в открытых публичных выступлениях, в т.ч. по радио, телевидению;
- потеря носителей информации.

К способам вывода из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи и систем обеспечения их функционирования, приводящим к уничтожению, искажению и блокированию, можно отнести:

- неправильный монтаж средств;
- поломку (разрушение) средств, в т.ч. разрыв (повреждение) кабельных линий связей;
- создание аварийных ситуаций для технических средств (поджог, искусственное затопление, взрыв и др.);
- отключение средств от сетей питания;
- вывод из строя или нарушение режима работы систем обеспечения функционирования средств;
- вмонтирование в электронную вычислительную машину (ЭВМ) разрушающих радио- и программных закладок;
- нарушение правил эксплуатации систем.

Способами нарушения режима работы технических средств отображения, хранения, обработки, воспроизведения, передача информации, средств связи и технологии обработки информации, приводящими к уничтожению, искажению и блокированию информации, могут быть:

- повреждение отдельных элементов средств;
- нарушение правил эксплуатации средств;
- внесение изменений в порядок обработки информации;
- заражение программ обработки информации вредоносными программами;
- выдача неправильных программных команд;
- превышение расчетного числа запросов;
- создание помех в радиоэфире с помощью дополнительного звукового или шумового фона, изменения (наложения) частот передачи информации;
- передача ложных сигналов – подключение подавляющих фильтров в информационные цепи, цепи питания и заземления;
- нарушение (изменение) режима работы систем обеспечения функционирования средств.

К видам дестабилизирующего воздействия на защищаемую информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи и систем обеспечения их функционирования относятся выход средств из строя; сбои в работе средств и создание электромагнитных излучений. Это приводит к уничтожению, искажению, блокированию, разглашению (соединение с номером телефона не того абонента, который набирается, или слышимость разговора других лиц из-за неисправности в цепях коммутации телефонной станции). Электромагнитные излучения, в том числе побочные, образующиеся в процессе эксплуатации средств, приводят к хищению информации.

К стихийным бедствиям и одновременно видам воздействия следует отнести землетрясение, наводнение, ураган (смерч) и шторм. К атмосферным явлениям (видам воздействия) относят грозу, дождь, снег, перепады температуры и влажности воздуха, магнитные бури. Они приводят к потере, уничтожению, искажению, блокированию и хищению.

Способами воздействия со стороны и стихийных бедствий и атмосферных явлений могут быть:

- разрушение (поломка);
- затопление;
- сожжение носителей информации, средств отображения, хранения, обработки, воспроизведения, передачи информации и кабельных средств связи, систем обеспечения функционирования этих средств;
- нарушение режима работы средств и систем, а также технологии обработки информации [2].

К причинам, вызывающим преднамеренное дестабилизирующее воздействие, следует отнести:

- стремление получить материальную выгоду (подзаработать);
- стремление нанести вред (отомстить) руководству или коллеге по работе;
- стремление оказать бескорыстную услугу приятелю из конкурирующей фирмы;
- стремление продвинуться по службе;
- стремление обезопасить себя, родных и близких от угроз, шантажа, насилия;
- физическое воздействие (побои, пытки) со стороны злоумышленника;
- стремление показать свою значимость.

Причинами непреднамеренного дестабилизирующего воздействия на информацию со стороны людей могут быть:

-неквалифицированное выполнение операций;
-халатность, безответственность, недисциплинированность, недобросовестное отношение к выполняемой работе;
-небрежность, неосторожность, неаккуратность;
- физическое недомогание (болезни, переутомление, стресс, апатия).

Причинами дестабилизирующего воздействия на информацию со стороны технических средств отображения, хранения, обработки воспроизведения, передачи информации и средств связи и систем обеспечения их функционирования могут быть:

- недостаток или плохое качество средств;

- низкое качество режима функционирования средств;
- перезагруженность средств;
- низкое качество технологии выполнения работ.

В основе дестабилизирующего воздействия на информацию со стороны природных явлений лежат внутренние причины и обстоятельства, неподконтрольные людям, а, следовательно, и не поддающиеся нейтрализации или устранению.

К числу наиболее вероятных каналов утечки информации можно отнести:

– совместную с другими фирмами деятельность, участие в переговорах;
– фиктивные запросы;
– посещения ЛПУ;
– общения представителей учреждения о характеристиках предоставляемых услуг;
– консультации специалистов со стороны, которые в результате этого получают доступ к установкам и документам фирмы;
– совещания, конференции и т.п.;
– разговоры в нерабочих помещениях;
– обиженных сотрудников фирм;
– технические каналы;
– материальные потоки (транспортировка спец почты).

При поликлиники защиты информации в медицинском учреждении необходимо учитывать следующие возможные методы и способы сбора информации:

– опрос сотрудников изучаемой учреждения при личной встрече;
– навязывание дискуссий по интересующим проблемам;
– ведение частной переписки со специалистами.

Для сбора сведений в ряде случае представители конкурентов могут использовать переговоры по определению перспектив сотрудничества, созданию совместных предприятий. Наличие такой формы сотрудничества, как выполнение совместных программ, предусматривающих непосредственное участие представителей других организаций в работе с документами, посещение рабочих мест, расширяет возможности для снятия копий с документов, сбора различных образцов материалов, проб и т.д. При этом с учетом практики развитых стран нарушители могут прибегнуть в том числе и к противоправным действиям, шпионажу.

Наиболее вероятно использование следующих способов добывания информации:

– визуальное наблюдение;
– подслушивание;
– техническое наблюдение;
– прямой опрос, выведывание;
– ознакомление с материалами, документами, изделиями и т.д.;
– сбор открытых документов и других источников информации;
– хищение документов и других источников информации;
– изучение множества источников информации, содержащих по частям необходимые сведения.

Изучив особенности расположения объекта и близлежащих зданий, можно представить возможные каналы утечки информации в виде таблицы (Таблица 1).

Таблица 1. Классификация возможных каналов утечки информации

Каналы утечки информации с объекта защиты		
1	Оптический канал	Окно помещения
2	Радиоэлектронный канал	ПЭВМ
		СИРД
		Телефон
		ВТСС
		ОТСС
		Система ОПС
		Система энергоснабжения и розетки
3	Акустический канал	Теплопровод подземный
		Водопровод подземный
		Стены помещения
		Система центрального отопления
		Вентиляция
4	Материально-вещественный канал	Документы на бумажных носителях
		Персонал предприятия
		Твердотельные накопители

Для исключения угроз утечки информации по техническим каналам следует внедрить систему комплексной защиты информации в медицинском учреждении.

В результате анализа можно сделать определенные выводы.

Для организации эффективной защиты от различных преднамеренных угроз необходимо четко представлять, что намеривается сделать злоумышленник. Для совершения преступления необходимо наличие одновременно трех составляющих – желания, способности и возможности. Соответственно, для предотвращения преступления необходимо убрать один из этих «необходимых, но недостаточных» элементов. Применяя КСЗИ разработанную для охраняемого объекта, можно существенно снизить или устранить две составляющие – желание и возможности.

References:

1. Методика моделирования угроз безопасности информации. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/ dokumenty/149-proekty.
2. Методика оценки угроз безопасности информации. 2021 год. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021