УДК 004.04

**ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ОБСЛУЖИВАЮЩЕЙ ОРГАНИЗАЦИИ.**

**Слесарева Алиса Михайловна**

Казанский национальный технологический исследовательский университет, Казань, Россия

a.mihailovna18@gmail.com

**Научный руководитель: к.т.н., доцент Алексеева А.А.**

***Аннотация.***В статье рассматривается защита информации, а именно персональных данных, в медицинских учреждениях. Раскрываются основные принципы, благодаря которым обеспечивается защита данных, а также представлены возможные методы ее улучшения и автоматизации. В результате исследования было проведено изучение системы защиты в медицинских организациях. Показано, что основные инциденты нарушения безопасности данных связаны низкой квалификацией персонала, отсутствием единой организационной системы защиты и контроля. Для решения данных задач требуется обновление программного обеспечения и четкое регулирование со стороны государственных органов.

***Ключевые слова:*** защита информации, персональные данные, защита персональных данных, обработка персональных данных, медицинская организация.

**PROTECTION OF PERSONAL DATA OF THE SERVICE ORGANIZATION.**

**Alisa M. Slesareva**

Kazan National Technological Research University, Kazan, Russia

a.mihailovna18@gmail.com

***Annotation.*** The article discusses the protection of information, namely personal data, in medical institutions. The basic principles by which data protection is ensured are revealed, and possible methods for its improvement and automation are presented. As a result of the study, a study of the protection system in medical organizations was conducted. It is shown that the main incidents of data security violations are associated with low qualifications of personnel and the lack of a unified organizational system of protection and control. To solve these problems, software updates and clear regulation by government agencies are required.

***Keywords:*** Information protection, рersonal information? protection of personal information; processing of personal data; medical organization.

Современные технологии и цифровизация привели к тому, что персональные данные стали одним из самых ценных активов для организаций. Обслуживающие компании, такие как банки, медицинские учреждения, интернет-провайдеры и другие, хранят и обрабатывают огромные объемы чувствительной информации о своих клиентах и поэтому защита персональных данных является для них важной задачей.

В соответствии с № 152 ФЗ «О персональных данных» (152-ФЗ) персональные данные представляют собой любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [1].

В медучреждениях обрабатываются два типа персональных данных (ПДн). Первый — простые данные: ФИО, дата и место рождения, рост, вес, фотографии, адрес, контактные данные. Второй — данные специальной категории: состояние здоровья, причины обращения, диагноз, лечение, объединенные под термином «врачебная тайна». Сохранность этих данных регулируется Федеральным законом № 323 от 21.11.2011, что делает проблему утечек информации особенно актуальной.

Согласно ФЗ-152, обработка ПДн включает: сбор, запись, систематизацию, накопление, хранение, обновление, извлечение, использование, передачу, обезличивание, блокирование, удаление и уничтожение, как с применением автоматизации, так и без нее. Перед получением информации от пациента, медицинская организация обязана получить его согласие на обработку ПДн в соответствии со статьями 6 и 10 упомянутого закона. Пациент имеет право отказаться от согласия полностью или частично. Поэтому при запросе данных медицинская организация должна ограничиться только необходимой информацией, соответствующей целям обработки и избежать избыточности в сборе (согласно статье 5 закона).

Медицинская организация обязана учитывать этические аспекты и обеспечивать безопасное хранение информации о здоровье пациентов, чтобы предотвратить утечку таких данных. В медицинской этике существуют правила, запрещающие разглашение определенных болезней, которые являются социально табуированными или приватными. Такие данные должны оставаться конфиденциальными согласно базовым принципам медицинской этики. [2].

Главный врач частных клиник и государственных больниц несет ответственность за безопасную обработку и хранение данных пациентов. Для этого выбирается подходящая медицинская информационная система и осуществляется контроль за защитой информации. Обработка информации о здоровье подчиняется строгим правилам, включая получение письменного согласия пациента, возможность доступа к данным по его инициативе, и использование данных в случае угрозы жизни или для медицинских целей. Врачебная тайна также защищена законом и не подлежит разглашению. [3].

При неотложно (экстренной) медицинской помощи согласие пациента на обработку его ПДн не требуется, а именно когда возникают техногенные катастрофы, стихийные бедствия, или когда имеется реальная угроза его жизни и здоровью. В настоящее время, с использованием современных информационных систем, обработка таких данных становится более удобной и безопасной. Это достигается за счет трех основных инструментов:

1. специализированные приложения с локальным или сетевым хранилищем;

2. медицинские информационные системы (МИС), работающие внутри конкретного медицинского учреждения;

3. облачные платформы для сбора и хранения информации.

Это означает, что при оказании экстренной помощи важно не замедлять процесс ожиданием согласия на обработку данных пациента. Современные информационные технологии позволяют эффективно управлять данными и обеспечивать их конфиденциальность в экстренных ситуациях. [4].

В случае срочной медицинской помощи согласие на обработку персональных данных не требуется при техногенных катастрофах, стихийных бедствиях или угрозе жизни и здоровью пациента. Использование современных информационных систем упрощает и обеспечивает безопасность обработки данных в медицинских учреждениях. Основные инструменты в этой области включают специализированные приложения, медицинские информационные системы (МИС) и облачные платформы. Более десяти лет назад Министерство здравоохранения и социального развития РФ разработало концепцию создания Единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ), но ее внедрение затрудняется из-за ограниченного технического оборудования в многих государственных медицинских центрах. В связи с этим вопросы обеспечения безопасности и хранения персональных данных рассматриваются индивидуально в каждом учреждении. [5].

Медицинские информационные системы (МИС) снижают риск взлома и утечки данных, но требуют ограничения доступа. Клиники должны внедрить пропускную систему, видеонаблюдение и многоуровневые пароли. Регулярное обучение персонала по законодательству обязательно. Проект защиты данных включает сбор информации, моделирование угроз, определение уровней защиты, разработку техзадания, проектирование системы защиты, создание документации, установку средств защиты и, опционально, аттестацию системы. Ошибки на любом этапе могут привести к серьезным последствиям и дополнительным расходам. Утечки могут повлечь административные и уголовные санкции для клиники и сотрудников. За нарушения могут быть наказаны и злоумышленники.

В связи с характером медицинских данных, кибербезопасность в здравоохранении стала уникальной задачей. На безопасность информации в здравоохранении также влияют недостаточные организационные меры по защите информации, отсутствие проверки соответствия требованиям информационной безопасности и нехватка по информационной безопасности и кибербезопасности.

Для обеспечения информационной безопасности необходимо не только установить комплексную систему, соответствующую стандартам, но и провести обучение персонала навыкам безопасного обращения с информацией. Важно осуществлять контроль за использованием данных, разработать протоколы реагирования на инциденты с четким определением ролей и обязанностей. Регулярная оценка рисков киберугроз также является ключевым моментом в поддержании информационной безопасности.

**Список источников**

1. Федеральный закон «О защите персональных данных» от 27.07.2006 №152-ФЗ.
2. Защита персональных данных в медицине: что нужно знать? // Центр безопасности данных : [сайт]. — URL: https://data-sec.ru/public/personal-data/zashchita-pdn-v-meditsine/
3. Антипов, А. А. Основы информационной безопасности / А. А. Антипов, А. А. Левин - 2021.
4. Защита персональных данных в медицинских учреждениях // SearchInform: [сайт]. — URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/perechen-personalnyh-dannyh-podlezhashchih-zashchite/zaschita-personalnykh-dannykh-v-meditsinskikh-uchrezhdeniyakh/
5. Персональные данные пациентов в медицинских организациях: требования к обработке и ответственность // Электронный Экспресс : [сайт]. — URL: https://www.garantexpress.ru/statji/personalnie-dannie-patsientov-v-meditsinskih-organizatsijah-trebovania-k-obrabotke-i-otvetstvennost/

**References**

1. Federal'nyy zakon «O zashchite personal'nykh dannykh» ot 27.07.2006 №152-FZ.
2. Zashchita personal'nykh dannykh v meditsine: chto nuzhno znat'? // Tsentr bezopasnosti dannykh : [sayt]. — URL: [https://data-sec.ru/public/personal-data/zashchita-pdn-v-meditsine/](https://vk.com/away.php?utf=1&to=https%3A%2F%2Fdata-sec.ru%2Fpublic%2Fpersonal-data%2Fzashchita-pdn-v-meditsine%2F)
3. Antipov, A. A. Osnovy informatsionnoy bezopasnosti / A. A. Antipov, A. A. Levin - 2021.
4. Zashchita personal'nykh dannykh v meditsinskikh uchrezhdeniyakh // SearchInform: [sayt]. — URL: [https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/perechen-personalnyh-dannyh-podlezhashchih-zashchite/zaschita-personalnykh-dannykh-v-meditsinskikh-uchrezhdeniyakh/](https://vk.com/away.php?utf=1&to=https%3A%2F%2Fsearchinform.ru%2Fresheniya%2Fbiznes-zadachi%2Fzaschita-personalnykh-dannykh%2Frealizaciya-zashchity-personalnyh-dannyh%2Fperechen-personalnyh-dannyh-podlezhashchih-zashchite%2Fzaschita-personalnykh-dannykh-v-meditsinskikh-uchrezhdeniyakh%2F)
5. Personal'nyye dannyye patsiyentov v meditsinskikh organizatsiyakh: trebovaniya k obrabotke i otvetstvennost' // Elektronnyy Ekspress : [sayt]. — URL: [https://www.garantexpress.ru/statji/personalnie-dannie-patsientov-v-meditsinskih-organizatsijah-trebovania-k-obrabotke-i-otvetstvennost/](https://vk.com/away.php?utf=1&to=https%3A%2F%2Fwww.garantexpress.ru%2Fstatji%2Fpersonalnie-dannie-patsientov-v-meditsinskih-organizatsijah-trebovania-k-obrabotke-i-otvetstvennost%2F)

**Информация об авторах**

А.М. Слесарева – студентка 2 курса специалитета, кафедры «Информационная безопасность».

А.А. Алексеева – кандидат технических наук, доцент;

**Information about the authors**

A.M. Slesareva is a 2nd year student of the specialty, Department of Information Security.

A.A. Alekseeva – candidate of technical sciences, associate professor;