МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра социальной информатики

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ ПО ДОКУМЕНТАМ ФСТЭК НА ПИМЕРЕ ОРГАНИЗАЦИИ ГКУЗ СО «СМЦМР «РЕЗЕРВ»

(автореферат бакалаврской работы)

студентки 5 курса 531 группы
направления 09.03.03 - Прикладная информатика
профиль Прикладная информатика в социологии
Социологического факультета
Петриченко Елизаветы Андреевны

Научный руководитель
старший преподаватель _____ М. В. Колесниченко
подпись, дата

Зав. кафедрой
кандидат социологических наук, доцент _____ И.Г. Малинский
подпись, дата

Саратов 2023

ВВЕДЕНИЕ

Актуальность темы обусловлена развитием новых информационных технологий, которые сопровождаются такими негативными явлениями, как промышленный шпионаж, компьютерные преступления и несанкционированный доступ (НСД) к информации. Сегодня одной из основных угроз безопасности информации является утечка информации по техническим каналам, несанкционированный доступ и непреднамеренные действия пользователей из-за недостаточных знаний в области информационной безопасности.

Создание Федеральной службы по техническому и экспортному контролю в России было непосредственно связано с растущей потребностью защиты информации. Указом Президента Российской Федерации от 16 августа 2004 года N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю"[1] была создана такая служба. Данное решение было вызвано быстрым развитием новых информационных технологий, которые в свою очередь увеличили количество негативных явлений, таких как промышленный шпионаж, компьютерные преступления и несанкционированный доступ к информации.

На сегодняшний день основной угрозой безопасности информации является происходящая утечка информации на техническом уровне, непреднамеренные действия пользователей и несанкционированный доступ. Данная проблема является невероятно актуальной в нашем обществе и требует внимания и мер предосторожности. В этом контексте Федеральная служба по техническому и экспортному контролю играет важную роль в области защиты персональных данных и другой важной информации.

Техническая защита информации в России является одной из ключевых областей обеспечения информационной безопасности. Это связано с тем, что с

[1] Указ Президента Российской Федерации от 16 августа 2004 г. N 1085 https://fstec.ru/dokumenty/vse-dokumenty/ukazy/ukaz-prezidenta-rossijskoj-federatsii-ot-16-avgusta-2004-g-n-1085 (Дата обращения 10.11.2022) Загл. с экрана. Яз. рус.

каждым годом количество компьютерных атак и компьютерных преступлений на территории России растет, а также с тем, что защита информации играет важную роль для государственной безопасности и экономики страны в целом.

Федеральная Служба по техническому и экспортному контролю (далее - ФСТЭК России) является органом государственной власти, который занимается регулированием отношений в области технической защиты информации. Документы, разработанные ФСТЭК России, определяют основные требования к защите информации и устанавливают правила и методы ее технической защиты.

Техническая защита информации в России с использованием документов ФСТЭК России является очень актуальной и важной задачей. Эти документы описывают требования к защите информации от несанкционированного доступа, утечки и изменения, а также устанавливают порядок проведения аудита технических средств защиты информации и установки их на объектах.

Кроме того, ФСТЭК России определяет требования к технической защите информации при использовании современных технологий, таких как облачные вычисления, мобильные приложения и интернет вещей. Это позволяет обеспечить защиту информации как на уровне отдельных компьютеров и сетей, так и на уровне крупных корпоративных систем и государственных информационных систем.

Таким образом, использование документов ФСТЭК России в области технической защиты информации является крайне актуальным в условиях растущей угрозы компьютерных преступностей и является одним из ключевых инструментов для обеспечения информационной безопасности в России.

Степень научной разработанности. Техническая защита информации является одной из наиболее важных областей в сфере информационной безопасности. Разработка и внедрение эффективных методов защиты информации являются зависимыми как от научных исследований, так и от практического опыта. Большое количество научных статей и исследований

было проведено в этой области, и ряд известных ученых внесли значительный вклад в ее развитие.

Среди ученых, которые занимаются исследованиями в области технической защиты информации, можно отметить, В.И. Васильева, В.А. Герасименко, А.А. Грушо, Е.Е. Тимонину, С.П. Расторгуева, А.Ю. Щербакова, Б. А. Погорелова, П. Н. Девянина, Д. И. Правикова, С. Н. Смирнова, Г.В. Фоменкова и др.

С.П. Расторгуев и А.Ю. Щербаков создали теорию разрушающих программных воздействий. Также А.Ю. Щербаков разработал принципиально новую субъектно-объектную математическую модель компьютерной безопасности, позволяющую обосновывать свойства защищенности компьютерных систем с точки зрения достаточных условий, в том числе разработка по проблематике разрушающих программных воздействий и безопасности распределенных компьютерных систем и сетей, математические модели «экономики знаний», исследование макроэкономической динамики в информационно-платежных системах нового поколения, работа в области теории распределенных реестров и цифровых активов.[1]

Важнейшим элементом деятельности В. А. Герасименко явилось формирование концепции и создание системы подготовки соответствующих специалистов, способных квалифицированно решать возникающие проблемы в условиях формирования информационного общества. Методист с большим опытом работы, В. А. Герасименко принял самое активное участие в разработке государственных образовательных стандартов, учебных планов и программ новой специальности «Комплексное обеспечение информационной безопасности автоматизированных систем». Им был разработан и реализован на практике целый ряд учебных курсов, в которых нашел отражение комплексный

[1] Биография Щербаков Андрей Юрьевич [Электронный ресурс] - URL: https://gubkin.ru/faculty/faculty-of-complex-safety-of-the-fuel-and-energy-complex/kafedry-i-podrazdeleniya/kbkvo/pps/sherbakov_a_u.php (дата обращения 26.05.2023) Загл. с экрана яз. рус.

подход, положенный в основу всей идеологии подготовки специалистов на кафедре.[1]

В проведенных исследованиях были рассмотрены различные аспекты технической защиты информации, включая области криптографии, стеганографии, систем ключей и аутентификации, беспроводных сетей, защиты компьютерных сетей и т.д. Большинство из этих исследований было опубликовано в научных журналах, таких как "Компьютерные инструменты в образовании", "Информатика и её применения", "Компьютерные науки и технологии", "Проблемы информационной безопасности" и других.

Цель бакалаврской работы – анализ применения руководящих документов ФСТЭК России по технической защите информации, а также оптимизация организационных и технических мероприятий по защите информации в ГКУЗ СО «СМЦМР «Резерв».

Задачи:

- Рассмотреть сущность понятия защиты информации

- Изучение содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

- Изучение требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;

- Рассмотрение политики обработки защищаемой конфиденциальной информации;

- Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных в ГКУЗ СО «СМЦМР «Резерв».

[1] Статья «К 80 - летию со дня рождения Владимира Андреевича Герасименко» [Электронный ресурс] - URL: https://bit.mephi.ru/index.php/bit/article/view/687/691# (дата обращения 26.05.2023) Загл. с экрана яз. рус.

Объектом работы является информационная инфраструктура организации ГКУЗ СО «СМЦМР «Резерв».

Предметом выступают угрозы, риски, возникающие в процессе реализации деятельности организации ГКУЗ СО «СМЦМР «Резерв».

В качестве **эмпирической базы** исследования были использованы нормативно-правовые документы ФСТЭК, Министерства здравоохранения, документы по защите информации ГКУЗ СО «СМЦМР «Резерв», облачные программы: СУОРД, УРМ, СУФД.

Теоретическая значимость подтверждается детальным рассмотрением перспектив использования документов ФСТЭК и оптимизации организационных и технических мероприятий на предприятиях и в учреждениях.

Практическая значимость исследования может быть проверена на практике и подтверждена путём внедрения в деятельность организаций.

Структура ВКР. Выпускная квалификационная работа состоит из списка обозначений и сокращений, введения, двух глав по три и пять параграфов соответственно, заключения и списка использованных источников.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе «Основные понятия информационной безопасности» рассматриваются такие понятия как понятия защита информации, несанкционированный доступ, угроза, уязвимость. А также раскрывается организация технической защиты информации в учреждении. Описываются вероятные источники угроз и способы их предотвращения.

Документация государственного регулирования устанавливает минимальные требования защиты от несанкционированного доступа к данным. Для противодействия киберугрозам ФСТЭК регулярно обновляет базу уязвимостей, вносит новые рекомендации в аттестацию, сертификацию оборудования, программного обеспечения.

В работе обозреваются цели и задачи ФСТЭК, а также основные законы, приказы, указы и постановления такие как:

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;

3. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»;

4. Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

5. Указ Президента Российской Федерации от 6 марта 1997 г. N 188 «Об утверждении Перечня сведений конфиденциального характера»;

6. Указ Президента Российской Федерации от 5 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

7. Указ Президента Российской Федерации от 2 июля 2021 г. N 400 «О стратегии национальной безопасности Российской Федерации»;

8. Приказ ФСТЭК России от 31 августа 2010 г. N 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»;

9. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

10. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

11. Методический документ. Утвержден ФСТЭК России 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»;

12. Методический документ. Утвержден ФСТЭК России 26 июня 2018 г. «Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в Банк данных угроз безопасности информации ФСТЭК России»;

13. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. «Методика оценки угроз безопасности информации»;

14. Методический документ. Утвержден ФСТЭК России 22 октября 2022 г. «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств»;

15. Методический документ. Утвержден ФСТЭК России 22 октября 2022 г. «Методика тестирования обновлений безопасности программных, программно-аппаратных средств»;

16. Национальный стандарт Российской Федерации. Защита информации. Термины и определения. ГОСТ Р 50922-2006.

Для того, чтобы система защиты информации грамотно работала необходимы продуманные и последовательные действия, а именно:

1. Проанализировать имеющиеся информационные ресурсы.
2. Подобрать концепцию ИБ, которая будет подходить по своей специфике и особенностям используемых данных.
3. Внедрить в систему средства защиты
4. Сформировать организационные меры защиты данных.[1]

Во второй главе «Защита информации в Государственном Казенном Учреждении Здравоохранения Саратовской области «Саратовский медицинский центр мобилизационных резервов «Резерв»» речь идет о

[1] Статья Техническая защита информации [Электронный ресурс] URL: https://imerk-security.ru/tekhnicheskaya-zashchita-informatsii (дата обращения 25.03.2023) загл. с экрана, яз. рус.

концепции защиты персональных данных, организационных и технических мерах защиты персональных данных, угрозах и уязвимостях безопасности, и контроле выполнения работ по обеспечению защиты персональных данных.

В соответствии с приказом министерства здравоохранения Саратовской области от 06.09.2021 ода № 2341 «Об эксплуатации системы «Система управления организационно-распорядительной документацией» в государственном казенном учреждении здравоохранения Саратовской области «Саратовский медицинский центр мобилизационных резервов «Резерв» организована автоматизированная система ведения документации по информационной безопасности.

Основными целями автоматизации мероприятий по организации информационной безопасности являются:

- повышение эффективности управления в сфере здравоохранения Саратовской области за счет повышения исполнительской дисциплины обеспечения прозрачности бизнес-процессов и использования инструментов контроля выполнения работ по подготовке организационно-распорядительной документации;
- внедрение системы управления организационно-распорядительной документацией (далее СУОРД);
- автоматизация средств защиты информации, включающих программно-аппаратные средства, средства антивирусной защиты и криптографической защиты от несанкционированного доступа, уничтожения, модификации и блокирования доступа к ней, а также от иных неправомерных действий в отношении такой информации;
- автоматизация процесса разработки и подготовки ОРД по организации информационной безопасности, в том числе по защите информации и обработке, и защите персональных данных для соответствия требованиям регуляторов Федеральной службы безопасности Российской Федерации, Роскомнадзора и ФСТЭК России;

- обеспечение готовности ОРД к проверкам регуляторов в сфере информационной безопасности;

Для обеспечения безопасности персональных данных применяются следующие организационные меры безопасности:

- инструктаж сотрудников по правилам обеспечения безопасности обрабатываемых персональных данных;
- учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;
- мониторинг и реагирование на инциденты информационной безопасности, связанные с персональными данными, включая проведение внутренних проверок, разбирательств и составление заключений;
- постоянный контроль за соблюдением требований по обеспечению безопасности персональных данных (реализуется путем внутренних аудитов);

ЗАКЛЮЧЕНИЕ

Техническая защита информации - это важная часть системы информационной безопасности. Она позволяет обеспечить защиту информации от несанкционированного доступа, изменения или уничтожения. С другой стороны, недостаточная защита информации может привести к утечке конфиденциальных данных, нанести ущерб имиджу компании, а также вызвать серьезные финансовые и юридические последствия.

Федеральная служба по техническому и экспортному контролю играет важную роль в области информационной безопасности России. Она отвечает за контроль за соблюдением требований в области технической защиты информации. Для этого ФСТЭК России проводит экспертизы, сертификации и аккредитации средств защиты информации, а также устанавливает требования к системам защиты персональных данных и информации, не отнесенной к государственной тайне.

Благодаря усилиям ФСТЭК России и других государственных органов в области информационной безопасности были созданы эффективные

инструменты защиты информации, которые широко используются в различных сферах бизнеса и государственном управлении. Важность ФСТЭК России в наше время заключается в том, что она позволяет обеспечить безопасность информации и защитить ее от угроз в реальном времени, способствуя сохранению конфиденциальности, целостности и доступности данных в целом.

Таким образом, в выпускной квалификационной работе (далее ВКР) в качестве теоретической основы были рассмотрены такие аспекты информационной безопасности как защита информации, несанкционированный доступ, угрозы и уязвимости. Также были подробно рассмотрены государственный орган ФСТЭК России его функции и задачи, принципы информационной безопасности, а именно конфиденциальность, целостность и доступность. Изучены организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Изучены требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

В ВКР были описаны организация технической защиты информации в организации, концепция защиты персональных данных, подробно описано проведение контрольных мероприятий и предоставлены перечни и актуальность угроз безопасности персональных данных в Учреждении

В выпускной квалификационной работе была рассмотрена конкретная государственная организация, один из отделов которой занимается формированием и обеспечением информационной безопасности персональных данных в Государственном Казенном Учреждении Здравоохранения Саратовской области «Саратовский медицинский центр мобилизационных резервов «Резерв».

В ходе выполнения ВКР были рассмотрены существующие меры по защите информации в Государственном Казенном Учреждении Здравоохранения Саратовской области «Саратовский медицинский центр мобилизационных резервов «Резерв».

В связи с санкционной политикой в отношении России для более качественной защиты информации требуется переход на отечественное программное обеспечение, особенно на операционные системы, хотя бы такие как Альт, РЕД ОС, Astra Linux, РОСА и чем быстрее это произойдет, тем безопаснее это для государственных учреждений.

Желательно приобрести на все АРМ средства защиты информации от несанкционированного доступа ПАК Аккорд, Dallas Lock, Secret Net Studio, VipNet, причем эти системы лучше иметь вместе с модулем обнаружения вторжений. Также с возросшим объемом работ необходимо ввести должность в штат Учреждения программиста или системного администратора.