ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.056.5:352.75

Особенности обеспечения информационной безопасности в районных администрациях

А.И. Дубровина, А.С. Казанцев
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
Процесс создания системы комплексной информационной безопасности (ИБ) является сложным и сопровождается необходимостью решения различных связанных с ней проблем. При этом актуальным является обеспечение безопасности и оценка уязвимостей автоматизированной информационной системы в аспекте надежности в условиях вредоносных воздействий. В настоящей работе проведен анализ особенностей обеспечения ИБ в районных администрациях, представлен комплекс мероприятий по улучшению системы.

Ключевые слова: информационная безопасность, районные администрации, внедрение ПО, обучение сотрудников

Для цитирования. Дубровина А.И., Казанцев А.С. Особенности обеспечения информационной безопасности в районных администрациях. *Молодой исследователь Дона.* 2024;9(3):36–39.

Features of Ensuring Information Security in District Administrations

Angelina I. Dubrovina, Aleksandr S. Kazantsev
Don State Technical University, Rostov-on-Don, Russian Federation

Abstract
The process of creating an integrated information security system is complex and requires solving various related problems. It is also important to ensure the reliability of an automated information system and assess its vulnerability to malicious influences. This paper analyzes the features of information security in district administrations and presents a set of measures to improve the system.

Keywords: information security, district administrations, software implementation, employee training

For citation. Dubrovina AI, Kazantsev AS. Features of Ensuring Information Security in District Administrations. *Young Researcher of Don.* 2024;9(3):36–39.

Введение. В Российской Федерации в органах местного самоуправления (МС) информационная деятельность ведётся исключительно на аппаратных средствах, использующих аттестованные в установленном порядке специальные программы. Большое внимание в данной ситуации необходимо уделять вопросам обеспечения информационной безопасности, сохранения конфиденциальной информации. Целью настоящей работы является разработка предложений по обеспечению и усилению защиты данных, хранимых в этих структурах. В рамках поставленной цели необходимо решить следующие задачи: провести аудит системы ИБ для выявления ее уязвимости, разработать и внедрить стратегию информационной безопасности, соответствующую особенностям работы районных администраций, обучить сотрудников правилам работы с конфиденциальной информацией, установить и поддерживать современные системы защиты информации (антивирусное программное обеспечение, межсетевые экраны, системы мониторинга и детекции вторжений), выявлять подозрительную активность и атаки в сетях, обеспечить строгий контроль доступа к информационным ресурсам с использованием аутентификации, авторизации и управления привилегиями, разработать и внедрить план действий в случае инцидентов, включая процедуры реагирования и восстановления.

Основная часть. Создание защиты. При выполнении данной работы авторы руководствовались следующими нормативными документами: приказ ФСБ России № 278 от 10.07.2014 [1], Федеральный закон № 149-ФЗ от 27.07.2006 [2], Федеральный закон № 152-ФЗ от 27.07.2006 [3], методический документ о мерах защиты информации в государственных информационных системах, утвержденный Федеральной службой по техническому и экспортному контролю [4].

На рис. 1 изображена схема служебного помещения, на которой показаны технические средства, предназначенные для обеспечения безопасности, датчики движения, системы пожаротушения, видеонаблюдения, охлаждения и бесперебойного питания, дверь с охранной сигнализацией и пропуском в серверное помещение.

Рис. 1. Схема служебного помещения

Авторами разработан комплекс локально-нормативных актов по обеспечению внутреннего трудового распорядка в области ИБ. Для достижения цели по улучшению информационной безопасности в зданиях районных администраций были определены следующие меры: разработаны общие положения, согласно которым сотрудникам необходимо соблюдать правила безопасности при работе с информацией во всех аспектах своей деятельности, знать политику обеспечения безопасности и процедуры ее соблюдения. Это относится к положениям или правилам в области информационной безопасности, которые предписывают сотрудникам соблюдать определенные стандарты безопасности в своей работе. Такие положения могут включать в себя требования по использованию безопасных паролей, ограниченному доступу к конфиденциальной информации, обязанности по информированию о потенциальных угрозах безопасности и т. д. Важно, чтобы сотрудники были ознакомлены с этими положениями и следовали им в своей повседневной деятельности [3].

К контролю доступа относится оснащение здания средствами, которые используются всеми сотрудниками при входе в здание и выходе из него (это могут быть как идентификационные карточки, беджи, электронные ключи, биометрические сканеры (например, сканеры отпечатков пальцев или сетчатки глаза), так и пин-коды или другие средства идентификации). Эти средства позволяют управлять доступом сотрудников в здание или в определенные помещения, обеспечивая безопасность и защиту конфиденциальных ресурсов.

Использовать информационные ресурсы сотрудники должны только в рамках своих служебных обязанностей, запрещается использование нелицензионного программного обеспечения. Также сотрудники должны соблюдать конфиденциальность информации и не разглашать её без соответствующего разрешения. Доступ к конфиденциальной информации должен быть предоставлен только сотрудникам, чьи должностные обязанности требуют такого доступа.

При обнаружении подозрительных вещей сотрудники должны немедленно сообщать об этом службе безопасности, а в случае инцидента необходимо следовать предписанным процедурам реагирования.

Меры системы менеджмента информационной безопасности, представленные на рис. 2, обеспечивают целостность, конфиденциальность и доступность информации в организациях, это позволяет эффективно защищать ресурсы районных администраций.

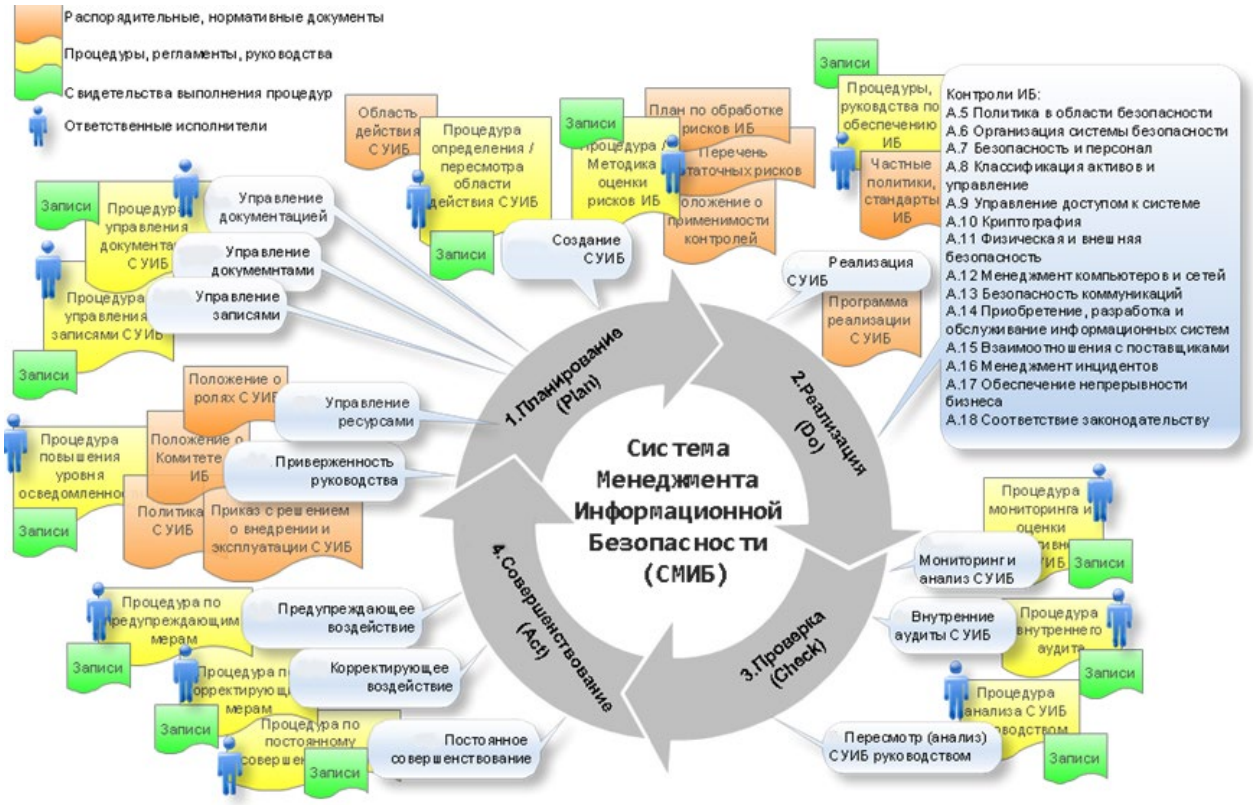

Рис. 2. Система менеджмента ИБ [5]

Каждый элемент в системе управления информационной безопасностью необходим для гарантии целостности, конфиденциальности и доступности информации в организации. Сотрудники службы безопасности устанавливают стандарты защиты информации и определяют обязанности сотрудников. Физическая безопасность — это защита физических ресурсов, включая контроль доступа и видеонаблюдение. Логическая безопасность — защита информации в электронной форме через шифрование и с помощью других технических средств. Управление рисками — разработка планов контингенции и аудиты безопасности. Обучение пользователей и мониторинг системы также играют важную роль в защите информации.

Заключение. В ходе данного исследования были предложены меры по обеспечению информационной безопасности в районных администрациях. Авторы подчеркивают необходимость обратить особое внимание на следующие аспекты при создании систем безопасности.

Во-первых, нужно разработать и принять предложения по соблюдению требований безопасности, сотрудники обязаны ознакомиться с проводимой в организации политикой информационной безопасности, а также ее процедурами, которые необходимо неукоснительно соблюдать в своей повседневной работе.

Во-вторых, ключевым моментом системы является контроль доступа к зданию или к определенным помещениям. Для этого используются различные средства идентификации, такие как идентификационные карточки, беджи, биометрические сканеры и т. д., которые обеспечивают аутентификацию сотрудников при входе и выходе.

Оперативно реагировать на угрозы и атаки на информационную систему помогают мониторинг и своевременное обнаружение инцидентов, что важно для предотвращения потенциальных утечек данных.

Все эти аспекты, задействованные в системе обеспечения информационной безопасности в районных администрациях, играют важную роль в создании надежного и защищенного окружения, способствуют эффективной работе организации и снижению рисков, связанных с утечкой или утратой конфиденциальной информации.

Список литературы

1. *Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности.* Приказ ФСБ России № 378 от 10.07.2014. URL: https://www.consultant.ru/document/cons_doc_LAW_167862/ (дата обращения: 05.03.2024).

2. *Об информации, информационных технологиях и о защите информации*. Федеральный закон № 149-ФЗ от 27.07.2006. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 05.03.2024).

3. *О персональных данных*. Федеральный закон № 152-ФЗ от 27.07.2006. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 05.03.2024).

4. *Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014)*. URL: https://www.consultant.ru/document/cons_doc_LAW_159975/ (дата обращения: 05.03.2024).

5. *ISO 27001/ГОСТ 27001-2013*. URL: https://realsec.ru/index.php/mn-services/mn-iso-27001 (дата обращения: 05.03.2024).

Об авторах:

Ангелина Игоревна Дубровина, ассистент кафедры вычислительных систем и информационной безопасности Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), adubrovina@yug.gkovd.ru

Александр Сергеевич Казанцев, студент кафедры вычислительных систем и информационной безопасности Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), aleks_kazanzev@mail.ru

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the Authors:

Angelina I. Dubrovina, Assistant of the Department of Computer Systems and Information Security, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), adubrovina@yug.gkovd.ru

Aleksandr S. Kazantsev, Bachelor's Degree Student of the Department of Computer Systems and Information Security, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), aleks_kazanzev@mail.ru

Conflict of interest statement: the authors do not have any conflict of interest.

All authors have read and approved the final manuscript.