УДК 004.056.5

Е. Г. Роскина [1], С. П. Серёдкин [1]

[1] Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННОГО УЧРЕЖДЕНИЯ

Аннотация. *Данная работа представляет собой подробное исследование процесса разработки политики безопасности для государственного учреждения. Описывается многоэтапный процесс, начиная от подготовительного этапа и анализа текущей ситуации по безопасности, и заканчивая мониторингом и аудитом политики после ее внедрения. Представлены ключевые аспекты, такие как определение требований к политике безопасности, разработка самого документа, утверждение и внедрение, а также постоянное обновление и улучшение в процессе деятельности. Особое внимание уделяется значению политики безопасности как основы для обеспечения конфиденциальности, целостности и доступности информации, а также минимизации угроз и рисков информационной безопасности учреждения. Данная статья может быть полезна с практической точки зрения для специалистов по информационной безопасности и руководителей государственных учреждений с целью обеспечения устойчивого функционирования учреждения.*

Ключевые слова: *политика безопасности, государственное учреждение, информационная безопасность, разработка, утверждение, внедрение, мониторинг*

E. G. Roskina[1], S. P. Seredkin [1]

[1] Irkutsk State University of Railway Engineering, Irkutsk, Russian Federation

DEVELOPING A SECURITY POLICY FOR A PUBLIC INSTITUTION

Abstract. *This paper is a detailed study of the security policy development process for public institutions. A multi-stage process is described, ranging from the preparatory phase and analysis of the current security situation to monitoring and auditing the policy after its implementation. Key aspects such as defining security policy requirements, developing the document itself, approval and implementation, and continuous updating and improvement are discussed. Emphasis is placed on the importance of the security policy as a framework for ensuring the confidentiality, integrity, and availability of information, as well as minimizing risks and threats to the institution. This paper is a valuable resource for information security professionals and managers of government agencies seeking to ensure robust information protection and sustainability of their organization.*

Keywords: *security policy, government agency, information security, development, approval, implementation, monitoring*

Введение

Создание и разработка политики безопасности для государственного учреждения представляет собой важный и сложный процесс, требующий глубокого понимания уникальных потребностей и угроз, с которыми сталкиваются такие организации. В современном мире, где информационные технологии играют ключевую роль в функционировании государственных институтов, обеспечение безопасности информации становится критической задачей. Политика безопасности является основой, на которой строится вся система защиты информации, и она должна охватывать широкий спектр аспектов, включая технические, организационные и правовые меры. В контексте государственных учреждений политика безопасности должна учитывать не только общепринятые стандарты и нормативы, но и специфические требования, вытекающие из характера и масштаба деятельности данного учреждения. Важно учитывать такие факторы, как важность и критичность обрабатываемой информации, потенциальные угрозы со стороны как внутренних, так и внешних злоумышленников, а также доступность и эффективность применяемых средств защиты информации.

Основные принципы разработки политики безопасности

Основная цель политики безопасности государственного учреждения состоит в обеспечении конфиденциальности, целостности и доступности информации, а также минимизации рисков от потенциальных угроз для нормального функционирования

организации [1]. Это требует не только разработки соответствующих правил и процедур, но и строгого выполнения сотрудниками учреждения установленных требований политики. Данное введение представляет лишь общий обзор темы разработки политики безопасности государственного учреждения и не охватывает всех аспектов этого сложного процесса [2]. Далее будет проведен детальный анализ основных принципов и методов разработки и реализации политики безопасности в контексте государственных структур.

Политика безопасности государственного учреждения — это комплекс правил, процедур и мероприятий, направленных на защиту информации, материальных ценностей, а также персонала учреждения от потенциальных угроз. Основная цель таких политик — обеспечение конфиденциальности, целостности и доступности данных, а также безопасности всех аспектов деятельности учреждения. Прежде всего, следует понимать, что политика безопасности государственного учреждения охватывают широкий спектр вопросов. Они включают в себя защиту информации от несанкционированного доступа, предотвращение утечек данных, защиту от кибератак, а также физическую защиту зданий и оборудования. Важной частью политики безопасности является управление доступом, что подразумевает установление четких правил, кто и в каких условиях может получить доступ к тем или иным ресурсам. Обычно этот процесс реализуется через системы контроля доступа, которые могут быть как программными, так и аппаратными. Включение механизмов двухфакторной аутентификации и биометрических данных является современным стандартом для обеспечения высокого уровня безопасности.

Другой важный аспект — это мониторинг и аудит безопасности. Государственное учреждение должно постоянно отслеживать свои информационные системы на предмет подозрительной активности и потенциальных угроз. Для этого используются системы обнаружения вторжений (IDS), антивирусные программы, фаерволы и другие средства защиты. Системность проведения аудитов безопасности, позволяет выявить уязвимости в системе защиты, программном обеспечении и предложить меры по их устранению. Важным элементом политики безопасности является план реагирования на инциденты. Это документ, в котором подробно описаны действия сотрудников при обнаружении нарушений безопасности, таких как утечка данных или кибератаки. План должен содержать четкие инструкции по изоляции угрозы, уведомлению ответственных лиц, восстановлению нормальной работы и проведению расследования инцидента.

Не менее важной является политика управления рисками. Государственное учреждение должно проводить регулярную оценку рисков, связанных с безопасностью, и принимать меры по их минимизации. Данный процесс включает в себя как технические меры, такие как установка обновлений и патчей, так и организационные меры, например, обучение персонала вопросам безопасности. Обучение и повышение осведомленности сотрудников является ключевым элементом успешной политики безопасности. Сотрудники должны быть ознакомлены с основными принципами защиты информации, правилами работы с конфиденциальными данными, методами предотвращения фишинга и социальной инженерии. Регулярные тренинги и учебные мероприятия помогут снизить вероятность человеческих ошибок, которые могут привести к серьезным нарушениям безопасности.

Физическая безопасность также играет важную роль в защите государственного учреждения. Она включает в себя контроль доступа к зданиям и помещениям, использование охранных систем, видеонаблюдения, а также меры по защите оборудования от краж и повреждений. Важным элементом является резервное копирование данных. Политика безопасности должна предусматривать регулярное создание резервных копий важных данных и их безопасное хранение. Эти действия необходимы для обеспечения возможности восстановления информации в случае ее утраты или повреждения.

Политика безопасности государственного учреждения должна быть адаптирована к специфическим условиям и требованиям каждой конкретной организации. Это включает в себя учет нормативных актов, стандартов и рекомендаций в области информационной безопасности, таких как ISO/IEC 27001, NIST и других. Важно также учитывать особенности

взаимодействия с другими государственными и частными организациями, включая вопросы обмена информацией и совместного использования ресурсов. В конечном итоге, успешная реализация политики безопасности зависит от вовлеченности и поддержки со стороны руководства учреждения. Политика безопасности должна быть неотъемлемой частью общей стратегии организации и поддерживаться на всех уровнях управления.

Таким образом, политика безопасности государственного учреждения представляют собой многоуровневую систему мер, направленных на защиту информации, ресурсов и персонала от различных угроз. Важными элементами этой системы являются управление доступом, мониторинг и аудит, план реагирования на инциденты, управление рисками, обучение сотрудников, физическая безопасность и резервное копирование данных. Политики безопасности должны быть гибкими и адаптивными, учитывающими специфические требования и условия каждой организации.

Этапы разработки политики безопасности

Разработка политики безопасности для государственного учреждения - это многоэтапный и комплексный процесс, начинающийся с анализа текущего состояния безопасности и заканчивающийся контролем и постоянным обновлением политики в соответствии с изменяющимся ландшафтом угроз. Основными этапами данного процесса являются:

1. Подготовительный этап. На этом этапе формируется команда, ответственная за разработку политики безопасности, а также определяются основные цели и задачи этого процесса [3].

2. Сбор информации. На этом этапе происходит сбор всей необходимой информации о системе безопасности учреждения, включая анализ существующих политик, процедур, технических средств защиты, а также оценку рисков и угроз.

3. Анализ информации. Построение модели угроз безопасности информации, анализ рисков [4].

4. Определение требований к политике безопасности. На основе результатов анализа формулируются основные требования, которым должна соответствовать политика безопасности, включая защиту конфиденциальности, целостности и доступности информации, а также минимизацию рисков.

5. Разработка политики безопасности. На этом этапе создается сам документ политики безопасности, включающий в себя определение целей, задач и принципов информационной безопасности, описание ролей и обязанностей сотрудников, процедур управления доступом, защиты информации и реагирования на инциденты [5].

6. Утверждение и внедрение. Политика безопасности должна быть утверждена руководством учреждения и внедрена в работу, а также должны быть предприняты меры по обучению сотрудников и обеспечению их соблюдения установленных правил и процедур.

7. Мониторинг и аудит. После внедрения политики безопасности необходимо осуществлять ее мониторинг и аудит с целью выявления возможных нарушений и несоответствий действующим требованиям законодательства, а также оценки эффективности принятых мер и необходимости их корректировки.

8. Обновление и улучшение. Требования политики безопасности должны быть актуальными, соответствовать реальной обстановке, соответствовать уровню развития информационных технологий, текущим угрозам безопасности и требованиям регуляторов.

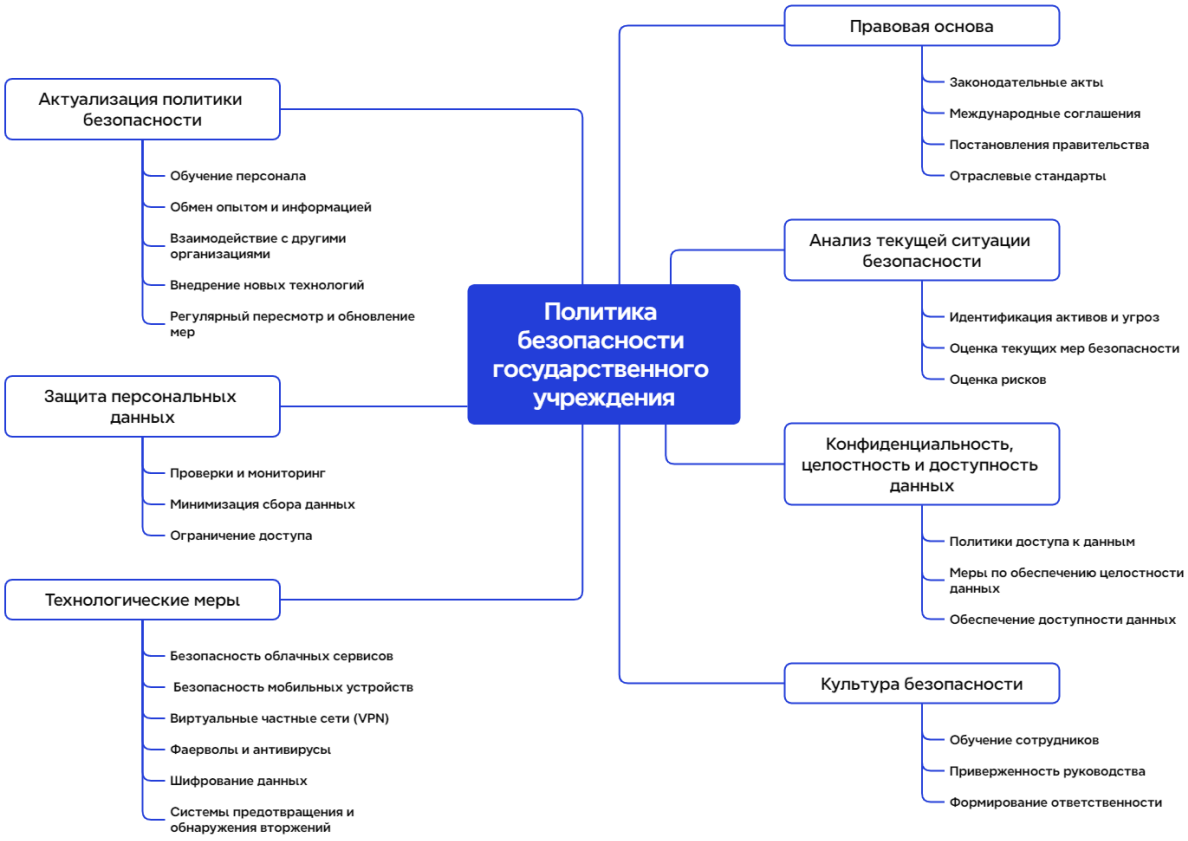

Рис. 1. Политика безопасности государственного учреждения

В разработке политики безопасности для государственного учреждения заложены основы обеспечения надежной защиты информации, которая является ключевым активом любой организации. Этот процесс представляет собой сложную систему мер и процедур, нацеленных на обеспечение конфиденциальности, целостности и доступности данных, а также минимизацию угроз и рисков. Важно понимать, что политика безопасности - это не просто документ на бумаге, а основа, на которой строится вся система защиты информации в учреждении. Ее эффективность зависит от тщательного анализа текущей ситуации безопасности, адекватной оценки угроз и рисков, а также строгого соблюдения установленных правил и процедур всеми сотрудниками и стейкхолдерами учреждения. Необходимо рассмотреть еще несколько важных аспектов, которые влияют на её эффективность и всесторонность. Одним из таких аспектов является правовая основа политики безопасности. Государственные учреждения действуют в рамках строгого регулирования и должны соблюдать требования нормативных актов и стандартов по защите информации. Эти требования могут включать законодательные акты, постановления правительства, методические документы ФСБ и ФСТЭК, отраслевые стандарты и международные соглашения. Соблюдение всех этих нормативных требований — критически важная часть политики безопасности, поскольку невыполнение их может привести к юридическим санкциям и потере доверия со стороны общественности и партнеров, санкциям со стороны регуляторов.

Важной частью реализации политики безопасности является создание и поддержка культуры безопасности внутри учреждения. Она включает в себя формирование у сотрудников понимания важности безопасности, их активное участие в выполнении мер безопасности и привитие ответственности за соблюдение установленных правил и процедур. Руководство должно демонстрировать приверженность вопросам безопасности, что может выражаться как в создании соответствующих условий и ресурсов для соблюдения политики, так и в личном примере. Технологические меры также играют ключевую роль в защите государственного учреждения. К ним относятся не только системы предотвращения и

обнаружения вторжений, фаерволы и антивирусы, но и современные технологии шифрования данных, использование виртуальных частных сетей (VPN), обеспечение безопасности мобильных устройств и облачных сервисов. В условиях растущей популярности удаленной работы и использования мобильных устройств важно обеспечивать безопасность доступа к корпоративным ресурсам из любых мест и устройств.

Особое внимание следует уделить защите персональных данных. Государственные учреждения работают с большим объемом персональной информации граждан, и утечка которых может привести к серьезным последствиям. Политики безопасности должны включать строгие меры по защите персональных данных, такие как минимизация сбора данных, ограничение доступа к ним, регулярные проверки и мониторинг использования данных. Важным аспектом является обеспечение безопасности передачи данных, что требует использования защищенных каналов связи и методов шифрования. Регулярное тестирование систем безопасности и проведение сценариев реагирования на инциденты — неотъемлемая часть поддержания высокого уровня безопасности. Оно позволяет выявлять потенциальные угрозы и уязвимости, проверять готовность сотрудников к действиям в критических ситуациях и совершенствовать существующие процедуры. Кроме того, проведение внешних аудитов и привлечение независимых экспертов позволяет получить объективную оценку уровня безопасности и определить необходимые направления для улучшения. В условиях быстро меняющейся технологической среды и появления новых угроз важно поддерживать политику безопасности в актуальном состоянии. Этот процесс требует регулярного пересмотра и обновления существующих мер и процедур, а также внедрения новых технологий и методов защиты. Важным элементом является взаимодействие с другими организациями и обмен опытом и информацией о современных угрозах и эффективных мерах их предотвращения. Киберугрозы становятся все более изощренными и разнообразными, поэтому эффективная политика безопасности должна быть многослойной и предусматривать различные уровни защиты. Такой процесс включает в себя как предотвращение атак на стадии их планирования, так и быстрое и эффективное реагирование на уже произошедшие инциденты. Политики безопасности должны учитывать и внутренние угрозы, которые могут исходить от сотрудников или подрядчиков учреждения. Это может быть вывано несанкционированным доступом к данным, нарушением правил безопасности или умышленными действиями. Для предотвращения таких угроз необходимо внедрять системы мониторинга и контроля за действиями сотрудников, проводить регулярные проверки и обучать персонал.

Разработка политики безопасности должна быть основана на принципах прозрачности, гибкости и постоянного совершенствования. Постоянное обновление и улучшение политики безопасности позволяет учреждению быть на шаг впереди потенциальных угроз и обеспечивать высокий уровень защиты информации. Эффективная политика безопасности государственного учреждения не может быть статичной, она должна развиваться вместе с изменяющейся внешней средой и внутренними процессами. Поэтому требуется постоянноый анализ новых угроз, адаптация к изменениям в законодательстве и технологиях, а также внедрению лучших практик и инновационных решений. Важным аспектом является также сотрудничество с другими государственными и частными организациями, участие в профессиональных сообществах и обмен опытом.

Заключение

Таким образом, проведенный анализ всех аспектов, учитывающихся при разработке политики безопасности, показал, что использование многоэтапного и комплексного подхода позволит значительно минимизировать вероятность реализации угроз и рисков информационной безопасности учреждения. При этом, в независимости от специфики деятельности конкретной организации обязательным условием устойчивого функционирования государственного учреждения в современном информационном обществе является внедрение многоуровневой системы мер, направленных на защиту информации, ресурсов и персонала.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Смотрицкая И. И., Черных С. И. Организационные инновации в сфере государственного управления //Вестник Института экономики Российской академии наук. – 2021. – №. 1. – С. 9-25.
2. Лепеш Г. В. Научно-техническая и технологическая безопасность Российской Федерации //Технико-технологические проблемы сервиса. – 2019. – №. 2 (48). – С. 3-8.
3. Ломазов В. А. и др. Применение сценарного подхода при разработке и прогнозировании результатов региональных программ развития агропромышленного комплекса //Инновации в АПК: проблемы и перспективы. – 2020. – №. 4. – С. 225-238.
4. Журавлева И. А. Оценка развития государственной образовательной политики (экспертный анализ) //Социология. – 2021. – №. 4. – С. 63-74.
5. Кузнецова Е. Экономическая безопасность и конкурентоспособность. Формирование экономической стратегии государства. – Litres, 2022. – 305 с.

REFERENCES

1. Smotritskaya I. I., Chernykh S. I. Organizational innovations in the field of public administration //Bulletin of the Institute of Economics of the Russian Academy of Sciences. – 2021. – №. 1. – Pp. 9-25.
2. Lepesh G. V. Scientific, technical and technological safety of the Russian Federation //Technical and technological problems of the service. – 2019. – №. 2 (48). – Pp. 3-8.
3. Lomazov V. A. et al. The use of a scenario approach in the development and forecasting of the results of regional programs for the development of the agro-industrial complex //Innovations in agriculture: problems and prospects. - 2020. – No. 4. – pp. 225-238.
4. Zhuravleva I. A. Assessment of the development of state educational policy (expert analysis) //Sociology. – 2021. – No. 4. – pp. 63-74.
5. Kuznetsova E. Economic security and competitiveness. Formation of the economic strategy of the state. – Litres, 2022. – 305 p.

Информация об авторах

Роскина Екатерина Григорьевна – студентка группы БИм.1-23, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: roskina26@gmail.com

Серёдкин Сергей Петрович - к. э. н., доцент кафедры «Информационные системы и защита информации» Иркутский государственный университет путей сообщения, г. Иркутск e-mail: seredkin_sp@irgups.ru

Information about the authors

Roskina Ekaterina Grigoryevna – student of the group BIm.1-23, Irkutsk State University of Railway Engineering, Irkutsk, e-mail: roskina26@gmail.com

Seredkin Sergey Petrovich – Candidate of Economic Sciences, Associate Professor of the Department of Information Systems and Information Protection, Irkutsk State Transport University, Irkutsk, e-mail: seredkin_sp@irgups.ru

Для цитирования

Роскина Е.Г., Серёдкин С.П. Разработка политики безопасности государственного учреждения // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2024. – №2. – С. 46-52. – Режим доступа: https://ismm.irgups.ru/toma/222-2024, свободный. – Загл. с экрана. – Яз. рус., англ.

For citations

Roskina E.G., Seredkin S.P. Developing a security policy for a public institution // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami:

ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2024. No. 2. P. 46-52.