УДК 004.056

ПРОБЛЕМЫ И ИХ РЕШЕНИЯ В ОБЛАСТИ ОРГАНИЗАЦИИ СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УПРАВЛЕНИЯ ПРОЕКТАМИ В ИБ

♦♦♦♦♦

ISSUES AND THEIR SOLUTIONS IN THE AREAS OF INFORMATION SECURITY SERVICE ORGANIZATION AND PROJECT MANAGEMENT

Диденко Данил Тарасович
магистрант,
Кубанский государственный технологический университет
didenko-d01@mail.ru

Аннотация. В статье рассмотрены проблематики в областях проектного управления в сфере информационной безопасностью и организации службы информационной безопасности. Были проанализированы существующие проблемы в каждой области и предложены практические решения для их устранения.

Ключевые слова: проектное управление, организация службы информационной безопасности, проектное внедрение, методы проектного управления.

Didenko Danil Tarasovich
Undergraduate Student,
Kuban State Technological University
didenko-d01@mail.ru

Annotation. The article examines the problems in the areas of project management in the field of information security and the organization of information security services. The existing problems in each area were analyzed and practical solutions for their elimination were proposed.

Keywords project management, information security service organization, project implementation, project management methods.

Введение

В современном мире информационная безопасность стала одним из ключевых аспектов деятельности любой организации, так как с развитием технологий возникают и новые угрозы. Это создает необходимость развития проектного управления в сфере информационной безопасности, чтобы эффективно защищать информацию. Однако, существует ряд проблем и сложностей, с которыми сталкиваются специалисты в области проектного управления в информационной безопасности. В данной статье мы рассмотрим основные проблемы, с которыми сталкиваются специалисты в данной области, а также возможные решения для эффективного управления проектами в сфере информационной безопасности.

Также стоит отметить, что на фоне роста угроз организация службы информационной безопасности тоже является важным аспектом работы любой компании, и решение проблем в этой области требует комплексного подхода. Знание существующих угроз, разработка четкой политики безопасности и обеспечение наличия квалифицированных специалистов являются основными шагами в улучшении ситуации в этой области. Это позволит компаниям защитить свои данные, минимизировать угрозы и обеспечить стабильную работу бизнеса. В данной статье мы рассмотрим ключевые проблемы организации службы информационной безопасности и предложим практические решения для их решения.

Так как данные проблематики актуальны и на сегодняшний день, то данная статья будет служить ресурсом для специалистов по информационной безопасности и управлению проектами, предоставляя полезные практические советы и решения для решения актуальных проблем в этих областях.

Проблемы в области проектного управления в информационной безопасности

В статье [1] автор приводит следующие ошибки в рамках проектной деятельности: ошибки в оценках, недостаточная мотивация, недостаточное тактическое планирование, ошибки декомпозиции, отсутствие гибкости. В статье [2] к основным проблемам применения проектного управления авторы относят нечеткое распределение функциональных обязанностей, недостаточную теоретическая подготовленность персонала и отсутствие формализации процессов проектного управления. Проанализировав статьи данных авторов, предложим решение проблем и рассмотрим подробно не-

которые из них. Также рассмотрим и другие некоторые проблемы, которые являются немаловажными.

Пожалуй, одной из основных и более важных проблем является отсутствие единой методологии для управления проектами в сфере информационной безопасности. Это создает сложности в планировании и выполнении задач, что может привести к уязвимостям и рискам для организации. Также стоит отметить, что проблема, с которой сталкиваются специалисты в области проектного управления в информационной безопасности, является сложность определения и управления рисками. Информационная безопасность подвержена множеству угроз, и специалистам необходимо уметь адекватно оценивать риски и разрабатывать эффективные стратегии и тактики их управления. Еще одной проблемой является недостаточная ясность в постановке задач и целей проекта. Часто бывает, что заказчик не до конца понимает свои потребности в области информационной безопасности, что затрудняет формирование четких и конкретных задач для проекта. Кроме того, часто возникают проблемы с неэффективным распределением ресурсов и управлением временем. В области информационной безопасности критически важно оперативно реагировать на угрозы и атаки, но нередко проекты не учитывают этот аспект, что приводит к потерям и срывам сроков. Также существует проблема отсутствия действенной системы управления проектами. В связи с этим, многие компании сталкиваются с проблемами в реализации проектов по обеспечению информационной безопасности, несвоевременным реагированием на киберугрозы и недостаточной готовностью к потенциальным кибератакам. Кроме того, недостаточная осведомленность сотрудников о важности информационной безопасности также является серьезной проблемой, с которой сталкиваются руководители проектов в данной области.

Решения для эффективного управления проектами в сфере информационной безопасности

Одним из основных методов решения проблем в области проектного управления в информационной безопасности является использование современных методик и методологий, таких как PRINCE2 (Projects IN Controlled Environments), PMBOK (Project Management Body of Knowledge), Agile и Scrum. Эти подходы позволяют оперативно реагировать на изменения в процессе выполнения проекта, что особенно важно в сфере информационной безопасности, позволяют эффективно планировать, контролировать и исполнять проекты. Кроме того, специалистам необходимо уделять большее внимание анализу и управлению рисками. Эффективное управление рисками позволит предотвратить негативные последствия и обезопасить проект от возможных угроз. Также важно уделять большое внимание постановке и формулировке целей проекта. Заказчику необходимо четко понимать, какие результаты проекта он ожидает, чтобы избежать недопониманий и недоразумений в процессе выполнения проекта. Наконец, эффективное распределение ресурсов и управление временем также играют важную роль в управлении проектами в сфере информационной безопасности. Специалисты должны уметь оптимально использовать имеющиеся ресурсы и оперативно реагировать на изменения в процессе выполнения проекта.

Также следует использовать следующие решения:

1. Регулярное обновление планов проекта: Учитывая быстрый темп изменений в технологиях и угрозах, необходимо регулярно обновлять планы проекта.

2. Создание мультидисциплинарных команд: Формирование команд, объединяющих экспертов по информационной безопасности, разработчиков и специалистов по управлению проектами, обеспечивает комплексный подход к решению задач проекта.

3. Опережающий анализ угроз: Применение методов прогнозирования и опережающего анализа угроз позволяет учитывать потенциальные угрозы и принимать меры еще до их актуализации.

Для более эффективного применения проектного управления в сфере информационной безопасности следует разработать единую методологию, которая будет упрощать работу при реализации проектов.

Проблемы в области организации службы информационной безопасности

Существует несколько основных проблем при организации службы информационной безопасности. Первая из них – это недостаток квалифицированных специали-

стов. Сфера кибербезопасности постоянно меняется, и многие компании испытывают трудности с поиском специалистов, обладающих актуальными знаниями и навыками. Специалисты, не обладающие достаточными знаниями и опытом, не могут обеспечить эффективную защиту системы от угроз. Согласно [3] **ИБ-специалисты госсектора сталкиваются дефицитом кадров в сфере ИТ и ИБ в 68 %**. Вторая проблема – это отсутствие четкой стратегии по защите информации и плана действий. Многие компании сталкиваются с тем, что служба информационной безопасности работает в изоляции от других подразделений организации и не имеет четких целей и задач, что приводит к разрозненной работе и недостаточной защите информации. Также они разрабатывают только базовые меры безопасности, что оставляет их уязвимыми перед современными угрозами. В статье [3] автор сообщает нам, что множество организаций имеют необходимость в разработке отдельных независимых от IT-стратегий ИБУР. И, наконец, третья проблема – это недостаток ресурсов. Многие компании не выделяют достаточно средств на развитие и поддержку службы информационной безопасности, на обновление оборудования, обучение сотрудников и мониторинг угроз, что также создает уязвимости. Также согласно [3] **нехватка финансирования для закупки необходимого ПО и оборудования составляет 64 %**.

Решения в области организации службы информационной безопасности

Для эффективной организации службы информационной безопасности необходимо обеспечить наличие квалифицированных специалистов. Специалисты в этой области должны иметь высокий уровень знаний и навыков, постоянно отслеживать изменения в угрозах и технологиях, и быть готовыми быстро реагировать на возникающие ситуации. Обучение и поддержка команды СИБ являются важным элементом в обеспечении безопасности информационных ресурсов. Это включает обучение существующих сотрудников и привлечение новых специалистов с необходимыми навыками. Также важно создать условия для удержания опытных специалистов, включая конкурентоспособную заработную плату и возможности для профессионального развития.

Важным аспектом организации службы информационной безопасности является также инвестирование в современные технологии и инструменты. Это может включать в себя внедрение мощных систем мониторинга и аналитики, использование средств идентификации и аутентификации, защиту от DDoS-атак и многое другое. Использование современных технологий поможет обеспечить более высокий уровень безопасности и защиты. Также необходимо увеличить осведомленность руководства компании о важности вопросов информационной безопасности и привлечение необходимых финансовых ресурсов. Это может быть достигнуто через проведение обучающих семинаров и презентаций, которые помогут продемонстрировать реальные угрозы и последствия нарушений безопасности.

Для решения проблемы отсутствия четкой стратегии и политики в области информационной безопасности необходимо разработать и внедрить комплексную программу, которая охватывает все аспекты безопасности информации. Это включает в себя аудит текущего состояния безопасности, разработку политики защиты информации, внедрение технических средств защиты и обучение сотрудников, правильно оценивать угрозы и уязвимости. Служба информационной безопасности должна тесно взаимодействовать с другими подразделениями компании, определять общие цели и задачи, и разрабатывать меры по защите информации.

Заключение

Информационная безопасность является одной из наиболее актуальных тем в современном мире. Проблемы, связанные с постоянно изменяющейся средой угроз, неосведомленностью сотрудников и отсутствием единой методологии для управления проектами, требуют серьезного внимания со стороны руководителей и специалистов по информационной безопасности. Развитие проектного управления в данной сфере позволит эффективно бороться с угрозами и рисками, обеспечивая высокий уровень защиты информации. Оно включает в себя управление рисками, оптимизацию расходов, планирование и мониторинг выполнения проектов и помогает компаниям добиваться максимальной эффективности в этой области. Использование современных методологий, постоянное обновление систем безопасности и повышение осведомленности сотрудников – вот основные меры, которые позволят достичь успеха в данной области.

Также организация службы информационной безопасности является важным аспектом работы любой компании, и решение проблем в этой области требует комплексного подхода. Понимание существующих угроз, разработка четкой политики безопасности и обеспечение наличия квалифицированных специалистов являются основными шагами в улучшении ситуации в этой области. Это позволит компаниям защитить свои данные, минимизировать угрозы и обеспечить стабильную работу бизнеса.

Литература

1. Мудунов А.С., Цахаева К.Н. Основные проблемы внедрения технологий проектного управления в российскую практику // Фундаментальные исследования. – 2015. – № 11-7. – С. 1457–1460.
2. Ошибки планирования в рамках стратегического управления проектами по информационной безопасности. – URL : https://lib.itsec.ru/articles2/control/oshibki-planirovan-v-ramkah-strategupravlen-proektami-po-informac-bezop
3. Дефицит кадров и финансирования – основные проблемы в формировании ИБ-инфраструктуры государственных организаций. – URL : https://www.comnews.ru/content/229100/2023-09-28/2023-w39/1010/deficit-kadrov-i-finansirovaniya-osnovnye-problemy-formirovanii-ib-infrastruktury-gosudarstvennykh-organizaciy?ysclid=lr9b7tyui6928077381
4. Разработка стратегии информационной безопасности и управления рисками. – Ч. 1. – URL : https://lib.itsec.ru/articles2/control/razrabotka-strategii-informacionnoi-bezopasnosti-i-ypravleniya-riskami-1
5. Оганесян Л.Л., Козырь Н.С. Проектное управление в информационной безопасности // Вестник Академии знаний. – 2023. – № 4.
6. A Guide to the Project Management Body of Knowledge, 2000 Edition. Newtown Square. PA: Project Management Institute. – 2000.
7. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности, – СПб. : СПбНИУИТМО, 2014. – 173 с.
8. David Alexander, Amanda Finch, David Sutton «Information Security Management Principles».
9. Krag Brotby, Gary Hinson «Information Security Governance: A Practical Development and Implementation Approach».
10. Susan Snedake «Information Security Project Management».

References

1. Mudunov A.S. The main problems of introducing project management technologies into russian practice / A.S. Mudunov, K.N. Tsakhaeva // Fundamental Research. – 2015. – № 11-7. – P. 1457–1460.
2. Planning errors in the framework of strategic information security project management. – URL : https://lib.itsec.ru/articles2/control/oshibki-planirovan-v-ramkah-strategupravlen-proektami-po-informac-bezop
3. Shortage of personnel and financing – the main problems in the formation of the information technology infrastructure of state organizations. – URL : https://www.comnews.ru/content/229100/2023-09-28/2023-w39/1010/deficit-kadrov-i-finansirovaniya-osnovnye-problemy-formirovanii-ib-infrastruktury-gosudarstvennykh-organizaciy?ysclid=lr9b7tyui6928077381
4. Development of an information security and risk management strategy. – Part 1. – URL : https://lib.itsec.ru/articles2/control/razrabotka-strategii-informacionnoi-bezopasnosti-i-ypravleniya-riskami-1
5. Oganesyan L.L. Project management in information security / L.L. Oganesyan, N.S. Kozyr // Bulletin of the Academy of Knowledge. – 2023. – № 4.
6. A Guide to the Project Management Body of Knowledge, 2000 Edition. Newtown Square. PA: Project Management Institute. – 2000.
7. Zhigulin G.P. Organizational and legal support of information security. – SPb. : SPbNIUITMO, 2014. – 173 p.
8. David Alexander, Amanda Finch, David Sutton «Information Security Management Principles».
9. Krag Brotby, Gary Hinson «Information Security Governance: A Practical Development and Implementation Approach».
10. Susan Snedake «Information Security Project Management».