УДК 004 **DOI: 10.18413/2518-1092-2024-9-1-0-3**

Федоров А.В.[1]
Жихарев А.Г.[2]
Кальченко Д.М.[1]

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ. ПРОБЛЕМЫ И РЕШЕНИЯ

[1)] Белгородский университет кооперации, экономики и права,
ул. Садовая, 116а, г. Белгород, 308023, Россия
[2)] Белгородский государственный технологический университет им. В.Г. Шухова,
ул. Костюкова, 46, Белгород, 308012, Россия

e-mail: zhikharev@bsu.edu.ru

Аннотация
В статье рассмотрены основные проблемы и соответственно принимаемые меры безопасности органов исполнительной власти, в которых определены цели и задачи, оценка рисков. Рассмотрены основные принципы выбора и внедрении защитных мер, разработки процедур и политик информационной безопасности, предложены основные отечественные системы управления информационной безопасностью, также описаны основные формы обучения сотрудников, мониторинга и принимаемых действий на основе анализа результатов мониторинга. Определены этапы анализа инцидентов в процессе расследования инцидентов, которые позволяют выявить уязвимости и проблемы в системе безопасности и принять меры по их устранению. Обусловлено регулярное обновление и совершенствование системы безопасности обеспечением более надежной защиты от различных видов угроз, приведено несколько рекомендаций для пересмотра и адаптации политик информационной безопасности с целью адаптация к изменяющимся условиям и требованиям. Приведены причины целесообразности внедрение систем управления информационной безопасности.
Ключевые слова: проблемы информационной безопасности; меры обеспечения; оценка рисков; защитные меры; системы управления информационной безопасности; мониторинг и анализ результатов; расследования инцидентов; уязвимости и проблемы; пересмотр и адаптация политик информационной безопасности; целесообразность внедрения систем управления информационной безопасности
Для цитирования: Федоров А.В., Жихарев А.Г., Кальченко Д.М. Обеспечение информационной безопасности в органах исполнительной власти. Проблемы и решения // Научный результат. Информационные технологии. – Т.9, №1, 2024. С. 19-28. DOI: 10.18413/2518-1092-2024-9-1-0-3

Fedorov A.V. [1]
Zhikharev A.G.[2]
Kalchenko D.M.[1]

ENSURING INFORMATION SECURITY IN EXECUTIVE AUTHORITIES. PROBLEMS AND SOLUTIONS

[1)] Belgorod University of Cooperation, Economics and Law,
116a Sadovaya str., Belgorod, 308023, Russia
[2)] Belgorod State Technological University named after V.G. Shukhov,
46 Kostyukova str., Belgorod, 308012, Russia

e-mail: zhikharev@bsu.edu.ru

Abstract
The article discusses the main problems and, accordingly, the security measures taken by executive authorities, which define goals and objectives, risk assessment. The basic principles of the choice and implementation of protective measures, the development of information security procedures and policies are considered, the main domestic information security management systems are proposed, the main forms of employee training, monitoring and actions taken based on the analysis of monitoring results are also described. The stages of incident analysis in the process of incident investigation are defined, which allow identifying vulnerabilities and problems in the security

system and taking measures to eliminate them. The regular updating and improvement of the security system is due to the provision of more reliable protection against various types of threats, several recommendations are given for the revision and adaptation of information security policies in order to adapt to changing conditions and requirements. The reasons for the expediency of implementing information security management systems are given.
Keywords: information security problems; security measures; risk assessment; protective measures; information security management systems; monitoring and analysis of results; investigation of incidents; vulnerabilities and problems; revision and adaptation of information security policies; the feasibility of implementing information security management systems
For citation: Fedorov A.V., Zhikharev A.G., Kalchenko D.M. Ensuring information security in executive authorities. Problems and solutions // Research result. Information technologies. – T.9, №1, 2024. – P. 19-28. DOI: 10.18413/2518-1092-2024-9-1-0-3

ВВЕДЕНИЕ

Обеспечение информационной безопасности (ИБ) является одним из ключевых аспектов современного мира, так как информация играет огромную роль в повседневной жизни людей, а также в деятельности предприятий и организаций. В условиях цифровой трансформации и активного использования информационных технологий, информационная безопасность становится особенно актуальной.

Проблемы ИБ связаны с угрозами нарушения конфиденциальности, целостности и доступности информации. Эти угрозы могут быть вызваны различными факторами, включая хакерские атаки, вирусы, фишинг, сбои в работе оборудования и программного обеспечения, а также человеческий фактор.

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение ИБ в органах исполнительной власти является одной из ключевых задач, так как от этого зависит конфиденциальность, целостность и доступность данных, а также защита от внутренних и внешних угроз. Однако, несмотря на все усилия и внедрение современных технологий, проблемы в области ИБ все еще остаются актуальными.

Проблемы ИБ можно разделить на несколько основных категорий:

- Недостаток квалифицированных специалистов: Проблема нехватки специалистов в области обеспечения ИБ актуальна для многих стран. Это связано с тем, что подготовка специалистов требует значительных временных и финансовых затрат, а также постоянного обновления знаний и навыков.
- Недостаточное финансирование: Недостаток средств на обеспечение ИБ может привести к тому, что меры по защите информации будут недостаточными или устаревшими. Это может привести к утечке конфиденциальной информации, нарушению работы информационных систем и другим негативным последствиям.
- Отсутствие единой стратегии: В разных органах исполнительной власти могут быть разные подходы к обеспечению ИБ, что может привести к несогласованности действий и снижению общего уровня защиты информации.
- Угрозы со стороны внешних источников: К ним относятся хакеры, киберпреступники и другие злоумышленники, которые могут использовать различные методы для получения доступа к конфиденциальной информации.

Одной из основных проблем, с которой сталкиваются органы исполнительной власти, является уязвимость информационных систем. Злоумышленники могут использовать различные методы, чтобы получить доступ к конфиденциальной информации. Это может привести к серьезным последствиям, таким как утечка данных, нарушение работы информационных систем и даже экономический ущерб.

МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для решения этой проблемы необходимо применять комплексные меры по обеспечению ИБ. Это включает в себя использование надежных методов шифрования данных, регулярное обновление программного обеспечения и операционных систем, а также обучение сотрудников правилам работы с конфиденциальной информацией.

К комплексным мерам по обеспечению ИБ относятся:

1. Определение целей и задач ИБ: На этом этапе разрабатывается стратегия по обеспечению ИБ. Определяются основные цели и задачи, такие как защита конфиденциальной информации, обеспечение доступности и целостности данных, предотвращение кибератак и т.д.

Обеспечение ИБ является одним из ключевых аспектов работы любой организации. Для эффективного управления рисками и обеспечения безопасности информации необходимо определить цели и задачи ИБ.

Цели информационной безопасности:

- Защита конфиденциальности: Обеспечение того, чтобы информация была доступна только авторизованным пользователям и не раскрывалась без разрешения.
- Защита целостности: Обеспечение точности, полноты и правильности информации, а также предотвращение ее несанкционированного изменения или уничтожения.
- Защита доступности: Обеспечение своевременного доступа к необходимой информации для авторизованных пользователей.
- Задачи информационной безопасности:
- Разработка и внедрение политики ИБ, которая устанавливает основные принципы и требования к обеспечению безопасности.
- Создание и поддержание системы управления ИБ (СУИБ), включая определение ролей и обязанностей, а также контроль за соблюдением политик ИБ.
- Внедрение мер и процедур для защиты информации от различных угроз, таких как вирусы, хакерские атаки, фишинг и т.д.
- Обучение и информирование сотрудников о мерах безопасности и их ответственности в области ИБ.
- Мониторинг и анализ системы ИБ с целью выявления уязвимостей и принятия мер по их устранению.
- Внедрение механизмов восстановления после инцидентов ИБ для минимизации их последствий.
- Взаимодействие с внешними организациями, такими как регуляторы, поставщики услуг и правоохранительные органы, по вопросам ИБ.
- Постоянное совершенствование системы ИБ и адаптация ее к изменяющимся условиям и угрозам.

2. Оценка рисков: Проводится анализ возможных угроз и уязвимостей, а также оценка рисков для информационных систем. Это помогает определить приоритетность мер безопасности и спланировать ресурсы для их реализации.

Оценка рисков включает в себя следующие этапы:

- Идентификация угроз: Определение возможных угроз для информационной системы, таких как хакерские атаки, вирусы, ошибки персонала и т. д.
- Оценка уязвимостей: Выявление слабых мест в системе, которые могут быть использованы угрозами для нарушения безопасности.
- Анализ рисков: Расчет вероятности реализации угроз и оценка возможных последствий для информационной системы.
- Выбор мер защиты: Определение оптимальных мер и средств защиты информации, направленных на минимизацию рисков.

• Мониторинг и аудит: Контроль за соблюдением мер защиты и анализ эффективности выбранных методов.

Оценка рисков может проводиться как на регулярной основе, так и при возникновении новых угроз или изменении условий работы информационной системы. Важно учитывать, что риски не являются статичными и могут изменяться в зависимости от внешних факторов и действий злоумышленников. Поэтому регулярная оценка и анализ рисков являются неотъемлемой частью обеспечения безопасности информационных систем.

3. **Выбор и внедрение защитных мер:** На основе проведенного анализа рисков выбираются соответствующие меры безопасности. Защитные меры могут включать в себя технические средства защиты, такие как антивирусное программное обеспечение, межсетевые экраны, системы обнаружения вторжений и т.д., а также организационные меры, такие как обучение персонала, контроль доступа к информации, регламентация работы с конфиденциальной информацией и т.п.

При выборе защитных мер необходимо учитывать множество факторов, таких как тип информационной системы, характер обрабатываемой информации, уровень угроз и уязвимостей, а также финансовые и технические возможности организации. Важно также обеспечить своевременное обновление и поддержку используемых защитных мер, чтобы они оставались эффективными и соответствующими современным угрозам.

Внедрение защитных мер должно осуществляться в соответствии с разработанной стратегией информационной безопасности, учетом требований законодательства и регуляторов. Необходимо также контролировать эффективность внедренных мер и при необходимости проводить их адаптацию и модернизацию.

В целом, выбор и внедрение защитных мер требует комплексного, профессионального подхода, чтобы обеспечить надежную защиту информации и минимизировать возможные риски для организации.

4. **Разработка процедур и политик ИБ:** Разрабатываются и документируются процедуры и политики, которые определяют порядок действий в случае инцидентов ИБ, правила работы с конфиденциальными данными, порядок реагирования на кибератаки и другие вопросы.

Процедуры ИБ могут включать в себя инструкции по работе с конфиденциальной информацией, правила использования информационных систем, процедуры реагирования на инциденты безопасности и т.д. Политики ИБ, в свою очередь, устанавливают общие принципы и направления деятельности организации в области информационной безопасности.

Разработка процедур и политик ИБ должна осуществляться с учетом специфики деятельности организации, ее информационных систем и существующих угроз. Важно также регулярно обновлять и актуализировать эти документы, чтобы они соответствовали текущим требованиям и стандартам безопасности.

Кроме того, процедуры и политики ИБ должны быть доступны для всех сотрудников организации и обязательны для исполнения. Это позволит обеспечить единый подход к обеспечению ИБ и снизить вероятность возникновения инцидентов.

5. **Внедрение системы управления ИБ:**

Существует несколько отечественных СУИБ, которые могут быть использованы в разных организациях в зависимости от их потребностей и специфики. Вот некоторые из них:

• АСТРА LINUX SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) – система, которая является частью операционной системы AstraLinux и обеспечивает мониторинг, сбор и анализ событий безопасности, а также обнаружение и предотвращение вторжений.“

• “DallasLock” – еще одна популярная российская СУИБ. Она обеспечивает защиту конфиденциальной информации и персональных данных, а также контроль доступа к информационным системам.

• “SecretNet” – программный комплекс для защиты информации от несанкционированного доступа, который включает в себя средства идентификации и аутентификации пользователей, шифрования данных и контроля целостности.

- "ЕЦУDallasLock" – современное сертифицированное на соответствие требованиям безопасности информации ФСТЭК России решение, которое находится в Едином реестре российских программ для ЭВМ и БД (№11185 от 29.07.2021 г.). Позволяет управлять не только различными СЗИ DallasLock, но также АРМами и серверами СЗИ DallasLock через Агента ЕЦУ для ОС Windows и Linux, позволяет контролировать сетевое оборудование, обеспечивает безопасный доступ к удаленному АРМ за пределами периметра организации. Лицензируется по количеству контролируемых АРМ и количеству сетевых устройств.
- "СЗИ DallasLockLinux" – специальная версия системы "DallasLock", предназначенная для защиты конфиденциальной информации в Linux-системах. (с 01.11.2023 г. прекращены продажи СБ DallasLock 8.0-С и 8.0-К – необходимо заменить на ЕЦУ DallasLock).
- "ParsecNet" – система контроля и управления доступом, которая обеспечивает безопасное удаленное подключение к корпоративным ресурсам.
- "SolarinRights" – решение для управления правами доступа к информационным ресурсам, позволяющее контролировать доступ к файлам, папкам, приложениям и другим объектам.
- "ZecurionDLP" – комплексная DLP-система последнего поколения. Защищает информацию от утечки по локальным и сетевым каналам, выявляет случаи корпоративного мошенничества, помогает расследовать инциденты и оценивать риски информационной безопасности.
- "InfoWatchTrafficMonitor" – программа для анализа и контроля информационных потоков в компании, выявления нарушений и инцидентов ИБ.
- "КриптоПроCSP, JCP, NETи т.д." – средства криптографической защиты информации.

Выбор СУИБ зависит от потребностей и возможностей конкретной организации. Некоторые из этих продуктов могут быть интегрированы друг с другом для обеспечения более комплексной защиты информации.

6. **Обучение и информирование сотрудников:** Сотрудники информируются о новых мерах безопасности и обучаются необходимым навыкам для работы с ними.

Обучение и информирование сотрудников является одним из ключевых аспектов управления персоналом. Оно способствует развитию профессиональных навыков, повышению квалификации, а также позволяет сотрудникам лучше понять цели и задачи компании, что в свою очередь положительно влияет на их мотивацию и лояльность.

Основные формы обучения сотрудников:

- Внутреннее обучение: включает проведение тренингов, семинаров, мастер-классов и других обучающих мероприятий внутри компании. Часто это наиболее экономичный вариант, так как не требует дополнительных затрат на внешние ресурсы.
- Внешнее обучение: предполагает привлечение внешних специалистов или организаций для проведения обучающих программ. Это может быть более дорогостоящим вариантом, но позволяет получить доступ к новым знаниям и технологиям.
- Онлайн-обучение: использование онлайн-платформ для дистанционного обучения, что позволяет сотрудникам обучаться в удобное для них время и месте.
- Наставничество: передача знаний и опыта от более опытных сотрудников к менее опытным, что помогает новичкам быстрее адаптироваться и развиваться в компании.

Информирование сотрудников включает в себя различные способы донесения информации до сотрудников. Это могут быть корпоративные рассылки, доски объявлений, встречи и совещания, а также корпоративная газета или журнал.

7. **Мониторинг и анализ системы безопасности**: Осуществляется постоянный мониторинг и анализ информационных систем на предмет потенциальных угроз и уязвимостей. Результаты мониторинга используются для корректировки и совершенствования системы ИБ.

Мониторинг и анализ систем безопасности является важной частью процесса обеспечения информационной безопасности предприятия. Это включает в себя наблюдение и сбор данных о состоянии безопасности информационных систем, сетей и оборудования, а также анализ этой информации для выявления потенциальных угроз и уязвимостей.

Мониторинг системы безопасности включает в себя:

- Обнаружение и предотвращение вторжений (IDS/IPS) – системы, которые отслеживают и анализируют сетевой трафик на предмет подозрительной активности.
- Системы обнаружения уязвимостей (VDMS) - программное обеспечение, которое сканирует системы на наличие известных уязвимостей и предоставляет отчеты об их состоянии.
- Системы мониторинга событий безопасности (SIEM) – инструменты, которые собирают, коррелируют и анализируют события безопасности из различных источников данных для выявления аномалий.
- Системы управления обновлениями (PatchManagement) – автоматизированные инструменты, которые следят за обновлениями и исправлениями для операционных систем и приложений, уведомляя пользователей о доступных обновлениях и помогая их применять.
- Системы анализа сетевого трафика – программное обеспечение для мониторинга сетевого трафика с целью выявления подозрительной активности или проблем.

Анализ данных мониторинга системы безопасности может включать такие действия, как:

- Идентификация и классификация угроз – выявление потенциальных угроз для информационных систем и определение их уровня риска.
- Определение уязвимостей - анализ данных мониторинга для обнаружения уязвимостей в системах и сетях, которые могут быть использованы злоумышленниками.
- Выработка рекомендаций по улучшению безопасности – на основе анализа данных мониторинга, предоставление рекомендаций по устранению уязвимостей, улучшению процессов безопасности и принятию превентивных мер.
- Управление инцидентами безопасности – обработка и реагирование на инциденты безопасности, включая сбор доказательств, расследование и восстановление после инцидентов.
- Анализ трендов и метрик – использование данных мониторинга для анализа тенденций и метрик, связанных с безопасностью, чтобы определить, какие области требуют улучшения или корректировок.
- Обучение и осведомленность – использование данных мониторинга и анализа для обучения сотрудников и повышения осведомленности о проблемах безопасности.

В целом, мониторинг и анализ системы безопасности является важным процессом, который помогает организациям обнаруживать и предотвращать угрозы, устранять уязвимости и улучшать общую информационную безопасность.

8. Расследование инцидентов ИБ: В случае возникновения инцидентов, проводится расследование для определения причин и принятия мер по их устранению.

В ходе расследования анализируются различные факторы, такие как действия злоумышленников, уязвимости в системе безопасности, ошибки персонала и другие факторы, которые могут привести к инцидентам.

Процесс расследования инцидентов включает в себя следующие этапы:

- Регистрация и классификация инцидентов: На этом этапе необходимо зарегистрировать все инциденты, связанные с информационной безопасностью, и классифицировать их по степени серьезности. Это поможет определить приоритеты и спланировать дальнейшие действия.
- Сбор и анализ информации: После регистрации инцидента необходимо собрать всю доступную информацию о нем, включая данные о злоумышленниках, используемых ими инструментах, методах атаки и других факторах. Анализ этой информации поможет выявить причины инцидента и определить меры, которые необходимо принять для его устранения.
- Определение причин инцидента: На основе собранной информации необходимо определить причины инцидента, включая уязвимости в системах безопасности, ошибки персонала или неправильные настройки. Это позволит принять меры для предотвращения подобных инцидентов в будущем.
- Разработка и реализация мер по устранению причин инцидента: После определения причин инцидента необходимо разработать и реализовать меры по их устранению. Эти меры могут

включать обновление программного обеспечения, изменение настроек системы, обучение персонала и другие действия.

- Мониторинг и контроль: После реализации мер по устранению причин инцидентов необходимо осуществлять мониторинг и контроль за их эффективностью. Это может включать в себя анализ логов системы безопасности, проведение регулярных аудитов и тестов на проникновение, а также оценку эффективности обучения персонала.
- Отчетность и информирование: По результатам расследования инцидентов необходимо подготовить отчет, в котором будут представлены все полученные данные, выводы и рекомендации. Этот отчет должен быть представлен руководству и другим заинтересованным сторонам, а также использован для информирования персонала о выявленных проблемах и мерах по их устранению.

Расследование инцидентов ИБ является важным компонентом системы обеспечения ИБ организации. Оно позволяет выявить уязвимости и проблемы в системе безопасности и принять меры по их устранению, что в свою очередь снижает вероятность возникновения подобных инцидентов в будущем.

9. Регулярное обновление и совершенствование системы безопасности: Система ИБ постоянно совершенствуется и обновляется с учетом новых угроз и технологических изменений. Может включать следующие пункты:

- Анализ уязвимостей: Регулярный анализ уязвимостей позволяет выявить слабые места в системе безопасности и принять меры по их устранению.
- Обновление программного обеспечения: Важно регулярно обновлять программное обеспечение, так как это снижает риск использования злоумышленниками уязвимостей.
- Обучение персонала: Сотрудники должны быть обучены работе с системами безопасности и знать, как правильно реагировать на различные угрозы.
- Внедрение новых технологий: Постоянное внедрение новых технологий может помочь улучшить систему безопасности и сделать ее более эффективной.
- Мониторинг и контроль: Системы мониторинга и контроля должны быть настроены для отслеживания активности пользователей и предотвращения возможных угроз.
- Установка антивирусного ПО: Установка антивирусного программного обеспечения и регулярное обновление его баз данных поможет защитить систему от вредоносных программ.
- Физическая безопасность: Обеспечение физической безопасности, например, установка систем видеонаблюдения, замков и охранных систем, поможет предотвратить несанкционированный доступ к системе.
- Разработка политик безопасности: Разработка и внедрение политик безопасности для всех пользователей системы поможет обеспечить соблюдение стандартов безопасности.
- Оценка рисков: Регулярная оценка рисков поможет определить наиболее уязвимые места и разработать стратегии для их устранения.
- Обратная связь: Получение обратной связи от пользователей и сотрудников позволит улучшить систему безопасности, учитывая их потребности и ожидания.

Регулярное обновление и совершенствование системы безопасности требует постоянных усилий и внимания, но в результате обеспечивает более надежную защиту от различных видов киберугроз и несанкционированного доступа к информации.

10. Пересмотр и адаптация политики ИБ: Периодически проводится анализ политики ИБ и ее адаптация к изменяющимся условиям и требованиям. Вот несколько рекомендаций для пересмотра и адаптации политик ИБ:

- **Регулярно проводите анализ рисков:** Оцените текущие угрозы и уязвимости в вашей организации, чтобы определить, какие изменения в политике ИБ необходимы.
- **Обучайте сотрудников:** Обучите всех сотрудников основам информационной безопасности, чтобы они знали, как правильно обращаться с конфиденциальной информацией и как реагировать на инциденты безопасности.

- **Внедрите новые технологии:** Постоянно следите за новыми технологиями и решениями в области ИБ, чтобы внедрять их в свою организацию.
- **Установите системы мониторинга и контроля:** Используйте системы мониторинга и контроля для отслеживания действий пользователей и обнаружения подозрительной активности.
- **Обновляйте программное обеспечение:** Регулярно обновляйте программное обеспечение на своих устройствах, чтобы устранить уязвимости и предотвратить атаки.
- **Обеспечьте физическую безопасность:** Обеспечьте надежную физическую безопасность, такую как установка систем видеонаблюдения и контроля доступа, чтобы предотвратить несанкционированный доступ в здание.
- **Разработайте политику паролей:** Разработайте и внедрите политику надежных паролей, чтобы предотвратить взлом учетных записей пользователей.

Проектируемая СУИБ должна соответствовать международным и отечественным стандартам ISO/IEC 27001:2022, ISO/IEC 27002:2022, NIST SP 800-53Rev.5, ГОСТ Р ИСО/МЭК 27001-2021, ГОСТ Р ИСО/МЭК 27002-2021, ГОСТ Р 59453.1-2021, ГОСТ Р 59453.2-2021. Одним из наиболее весомых факторов, которые необходимо учесть внес Указ Президента РФ от 01.05.2022 N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации". Он определяет построение СУИБ, а именно с 01.01.2025 г. использование иностранных средств защиты информации будет невозможно.

Внедрение СУИБ является целесообразным по следующим причинам:

- Защита данных: СУИБ обеспечивает защиту конфиденциальных данных от несанкционированного доступа, кражи, потери и других угроз, что позволяет сохранить целостность и доступность информации.
- Соответствие стандартам: Внедрение СУИБ помогает организациям соответствовать требованиям международных стандартов и регулятивных норм, таких как ISO 27001, PCI DSS, GDPR и другие, что снижает риск штрафов и судебных исков.
- Управление рисками: Система управления позволяет идентифицировать, анализировать и оценивать риски информационной безопасности, а также разрабатывать и внедрять соответствующие меры защиты. Это помогает организациям управлять рисками и предотвращать возможные инциденты информационной безопасности.
- Улучшение процессов: Система управления предоставляет инструменты для оптимизации процессов информационной безопасности, например, для определения политик и процедур, обучения персонала, мониторинга и аудита. Это способствует улучшению общего управления и контроля над информационной безопасностью организации.
- Повышение доверия клиентов и партнеров: Наличие СУИБ демонстрирует клиентам и партнерам организации высокий уровень профессионализма и надежности, что может способствовать увеличению доверия и улучшению отношений.
- Повышение конкурентоспособности: Внедрение современных СУИБ может дать организации конкурентные преимущества на рынке, так как это позволяет быстрее реагировать на угрозы и лучше адаптироваться к изменениям в отрасли.

ЗАКЛЮЧЕНИЕ

Таким образом, внедрение СУИБ приводит к улучшению контроля над информационными активами, снижению рисков и повышению уровня защиты конфиденциальных данных. Это, в свою очередь, способствует повышению конкурентоспособности, улучшению отношений с клиентами и партнерами, а также соблюдению требований регулятивных органов.

Внедрение СУИБ является целесообразным и актуальным для любой организации, поскольку позволяет обеспечить защиту конфиденциальной информации, улучшить процессы безопасности, соответствовать стандартам и минимизировать риски. Эта система помогает управлять рисками, улучшать процессы, повышать доверие клиентов и партнеров, а также повышать конкурентоспособность компании. В целом, внедрение СУИБ приводит к улучшению защиты

информационных активов и снижению рисков, что положительно сказывается на деятельности организации.

Список литературы

1. IT-специалисты в сфере информационной безопасности в 2022. − URL: https://habr.com/ru/articles/679086/. – [Электронный ресурс].

2. Кибербезопасность в 2022–2023. Тренды и прогнозы− URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/#id2. – [Электронный ресурс].

3. Фонд содействия развитию безопасных информационных технологий. Добро пожаловать, сеньоры! Рынок труда в сфере кибербезопасности в третьем квартале 2023 года − URL: https://fsrbit.ru/post/2132. – [Электронный ресурс].

4. Удовиченко А. Стратегия ИБ: а вы решили, как двигаться вперед? – 27.02.2019 г. − URL: https://habr.com/ru/companies/softline/articles/441920/. – [Электронный ресурс].

5. Модель безопасности AstraLinux — основа для апробации новых ГОСТов – 14.05.2021 г.− URL: https://astralinux.ru/about/press-center/news/model-bezopasnosti-astra-linux-osnova-dlya-aprobatsii-novykh-gostov/. – [Электронный ресурс].

6. Шиляев С. Проблемы информационной безопасности: алгоритм построения системы ИБ с нуля – 24.02.2015 г. − URL: https://kontur.ru/articles/1622 – [Электронный ресурс].

7. Реестр программного обеспечения. Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. − URL: https://reestr.digital.gov.ru/. [Электронный ресурс].

8. Указ Президента Российской Федерации от 01.05.2022 г. № 250О дополнительных мерах по обеспечению информационной безопасности Российской Федерации. − URL: http://www.kremlin.ru/acts/bank/47796. – [Электронный ресурс].

9. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. N 1653-ст. − URL: https://garant.belregion.ru/#/document/403510768/paragraph/764/doclist/32/showentries/0/highlight/ГОСТ%20Р%20ИСО%7СМЭК%2027001-2021:2. – [Электронный ресурс].

10.ГОСТ Р ИСО/МЭК 27002-2021. Методы и средства обеспечения безопасности. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности: издание официальное: утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. N 416-ст. − URL: https://garant.belregion.ru/#/document/402878331/paragraph/1/doclist/33/showentries/0/highlight/ГОСТ%20Р%20ИСО%7СМЭК%2027002-2021:4. – [Электронный ресурс].

References

1. IT specialists in the field of information security in 2022. − URL: https://habr.com/ru/articles/679086/. – [Electronic resource].

2. Cybersecurity in 2022-2023. Trends and forecasts − URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/#id2. – [Electronic resource].

3. Foundation for the Promotion of Secure Information Technologies. Welcome, senors! Cybersecurity labor market in the third quarter of 2023. − URL: https://fsrbit.ru/post/2132. – [Electronic resource].

4. Udovichenko A. IB strategy: have you decided how to move forward? – 02/27/2019 − URL: https://habr.com/ru/companies/softline/articles/441920/. – [Electronic resource].

5. AstraLinux security model — the basis for testing new GOST standards – 05/14/2021− URL: https://astralinux.ru/about/press-center/news/model-bezopasnosti-astra-linux-osnova-dlya-aprobatsii-novykh-gostov/. – [Electronic resource].

6. Shilyaev S. Problems of information security: algorithm for building an information security system from scratch – 02/24/2015. − URL: https://kontur.ru/articles/1622. – [Electronic resource].

7. Software registry. Ministry of Digital Development, Communications and Mass Communications of the Russian Federation. − URL: https://reestr.digital.gov.ru/. [Electronic resource].

8. Decree of the President of the Russian Federation No. 250 of 01.05.2022 on additional measures to ensure information security of the Russian Federation. − URL: http://www.kremlin.ru/acts/bank/47796. – [Electronic resource].

9. GOST R ISO/IEC 27001-2021. Information technology. Methods and means of ensuring security. Information security management systems. Requirements: national standard of the Russian Federation: official publication: approved and put into effect by the order of the Federal Agency for Technical Regulation and Metrology dated November 30, 2021 N 1653-st. − URL: https://garant.belregion.ru/#/document/403510768/paragraph/764/doclist/32/showentries/0/highlight/ГОСТ%20Р%20ИСО%7СМЭК%2027001-2021:2. – [Electronic resource].

10.GOST R ISO/IEC 27002-2021. Methods and means of ensuring security. Information technology. Methods and means of ensuring security. Code of Norms and Rules for the application of information security measures: official publication: approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated May 20, 2021 N 416-art. − URL: https://garant.belregion.ru/#/document/402878331/paragraph/1/doclist/33/showentries/0/highlight/ГОСТ%20Р%20ИСО%7СМЭК%2027002-2021:4. – [Electronic resource].

Федоров Алексей Васильевич, магистрант 2 курса кафедры информационная безопасность
Жихарев Александр Геннадиевич, доктор технических наук, доцент, доцент кафедры программного обеспечения вычислительной техники и автоматизированных систем
Кальченко Даниил Михайлович, магистрант 2 курса кафедры информационная безопасность

Fedorov Alexey Vasilyevich, 2nd year Master's student, Department of Information Security
Zhikharev Alexander Gennadievich, Doctor of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Engineering and Automated Systems Software
Daniil Mikhailovich Kalchenko, 2nd year Master's student, Department of Information Security