|  |
| --- |
| МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  Федеральное государственное автономное образовательное учреждение  высшего профессионального образования  **«Дальневосточный федеральный университет»** |
| **Институт математики и компьютерных технологий**  **Департамент информационной безопасности** |
| РЕФЕРАТ  по дисциплине «информационные технологии»  по направлению подготовки «Б9122-10.03.01 информационная безопасность»  образовательная программа «организация и технологии защиты информации в сфере коммерческой деятельности»  на тему «Системы защиты информации» |
| Выполнили студенты  Вернер Владимир Сергеевич  Чернухина Кристина Сергеевна  Проверил  Гореликов Роман Станиславович |
| г. Владивосток  2024 |

**Оглавление**

Введение 3

1 Классификация систем защиты информации

1.1 Программные системы защиты информации 4

1.2 Аппаратные системы защиты информации 5

1.3 Физические системы защиты информации 6

1.4 Организационные системы защиты информации 6

1.5 Социальные системы защиты информации 8

2 Недостатки систем защиты информации

2.1 Недостатки программных систем защиты информации 9

2.2 Недостатки аппаратных систем защиты информации 9

2.3 Недостатки физических систем защиты информации 10

2.4 Недостатки организационных систем защиты информации 10

2.5 Недостатки социальных систем защиты информации 11

3 Способы и методы минимизации и устранения недостатков систем защиты информации

3.1 Минимизация расходов 12

3.2 Комплексный подход 13

Заключение 14

Список использованных источников 15

**Введение**

Целью данной работы является приобретение практических и теоретических навыков по специальности, развитие навыков по работе с информацией и расширение знаний в области систем защиты информации предприятий для разработки перечня мероприятий по устранению и ограничению недостатков систем защиты информации предприятий и выработки предложений о возможности внедрения дополнительных мер.

Основные задачи:

– Ознакомиться с классификацией систем защиты информации предприятий;

– Выявить наиболее распространённые среди предприятий системы защиты информации;

– Изучить недостатки данных систем защиты информации;

– Изучить существующие методы устранения и ограничения недостатков систем защиты информации;

– Разработать перечень наиболее эффективных мероприятий по устранению и ограничению недостатков;

– Выработать предложения о возможности внедрения дополнительных мер.

**1 Классификация систем защиты информации**

**1.1 Программные системы защиты информации**

Среди программных систем защиты информации можно выделить:

– антивирусные программы: обнаруживают, блокируют и удаляют вредоносные программы, такие как вирусы, трояны и черви. Они обеспечивают защиту от потенциальных угроз для системы и данных.

– брандмауэры: контролируют входящий и исходящий сетевой трафик и применяют различные политики безопасности для защиты сети от несанкционированного доступа.

– антишпионские программы: обнаруживают и удаляют шпионское программное обеспечение, которое может собирать информацию о пользователе и его активностях без его согласия.

– средства контроля доступа: ограничивают доступ к информации или ресурсам только авторизованным пользователям, используя различные механизмы аутентификации и авторизации.

– криптографические программы: обеспечивают безопасность данных путем их зашифрования. Они используют различные алгоритмы и ключи для обеспечения конфиденциальности и целостности информации.

Программными системами защиты информации являются специальные комплексные программные решения, которые предназначены для защиты информации от несанкционированного доступа, утечки и незаконного использования. Они содержат в себе различные механизмы и инструменты, которые обеспечивают конфиденциальность, целостность и доступность информации.

Программные системы защиты информации предлагают комплексное решение для защиты данных организации. Они включают в себя различные методы и технологии, которые помогают предотвратить несанкционированный доступ к конфиденциальной информации.

Одним из главных преимуществ программных систем защиты информации является их гибкость. Они могут быть настроены на различные типы и уровни защиты в зависимости от потребностей организации. Это позволяет предоставить только необходимый доступ к информации, минимизирует риски утечки данных и повышает уровень безопасности.

Вторым полезным аспектом программных систем защиты информации является возможность управления доступом. Пользовательские права и настройки могут быть определены для каждого пользователя или группы пользователей, что позволяет контролировать и ограничивать доступ к конфиденциальной информации.

Системы защиты информации также обеспечивают отчетность о событиях, связанных с безопасностью данных. Они предоставляют отчеты о входах и выходах пользователей, а также обнаруживают попытки несанкционированного доступа. Это помогает предотвратить потенциальные проблемы и повысить эффективность системы защиты информации.

**1.2** **Аппаратные системы защиты информации**

К программным системам защиты информации относятся следующие устройства:

– биометрические устройства: используют уникальные физиологические или поведенческие характеристики пользователя, такие как отпечатки пальцев, голос или сетчатка глаза, для аутентификации и контроля доступа.

– устройства аутентификации: позволяют пользователям подтверждать свою личность, используя различные методы, такие как PIN-коды, токены или смарт-карты.

– средства хранения информации с защитой: обеспечивают безопасное хранение данных с использованием различных механизмов шифрования и защиты от физического или логического вторжения.

– устройства безопасной передачи данных: обеспечивают безопасную передачу данных через сеть, предотвращая их перехват, модификацию или подделку.

Аппаратными системами защиты информации являются комплексы технических средств, включающих в себя аппаратное обеспечение и специализированные устройства (например, программируемые контроллеры доступа, межсетевые экраны), предназначенный для защиты информации от несанкционированного доступа, повреждения, утечки или других угроз.

Аппаратные системы защиты информации обладают рядом преимуществ, которые обусловливают их популярность и широкое применение в сфере информационной безопасности.

Во-первых, аппаратные системы обеспечивают высокий уровень защиты информации. Они способны надежно защищать данные от взломов, вирусов, атак хакеров и других потенциальных угроз. Ключевым преимуществом аппаратных систем является то, что они работают на физическом уровне, что делает их более надежными и устойчивыми к атакам.

Во-вторых, аппаратные системы обладают высокой производительностью. Они способны обрабатывать большие объемы данных и выполнять сложные операции без серьезного снижения производительности компьютерной системы. Это особенно важно для предприятий, где присутствует значительный поток информации, требующий непрерывной и быстрой обработки.

Третье преимущество аппаратных систем заключается в их независимости от программного обеспечения. Защита данных осуществляется на уровне аппаратного обеспечения, что делает системы независимыми от программного обеспечения и операционной системы. Это позволяет использовать аппаратные решения с любыми операционными системами и гибко настраивать их работу в соответствии с требованиями организации.

Наконец, аппаратные системы обладают удобством использования. Большинство таких систем имеют интуитивно понятный интерфейс и простую установку, что облегчает их внедрение и использование даже для непрофессионалов. Это позволяет организациям быстро внедрять защиту и обеспечивать безопасность своих данных.

**1.3** **Физические системы защиты информации**

Среди физических систем защиты информации можно выделить:

– охранные системы: обеспечивают контроль и мониторинг безопасности помещений или зданий.

– датчики дверей и окон: обнаруживают несанкционированное открытие дверей или окон и активируют сигнал тревоги или уведомления.

– системы контроля доступа: ограничивают или регулируют доступ к зданию или помещению, используя различные методы, такие как электронные ключи, кодовые карты или биометрические данные.

– сейфы и трезоры: обеспечивают безопасное хранение ценных предметов или документов с использованием механических или электронных механизмов блокировки.

Физическими системами защиты информации являются технические меры и средства, предназначенные для обеспечения физической безопасности информации и инфраструктуры, на которой она хранится или передается.

Преимущества физических систем защиты информации:

– физические системы защиты предоставляют дополнительный уровень безопасности, обеспечивая защиту от несанкционированного доступа физических лиц к компьютерным системам и данным. Это особенно важно для организаций, хранящих конфиденциальную информацию или личные данные своих клиентов.

– они обеспечивают защиту от физических угроз, таких как кража оборудования или несанкционированный доступ к серверам. Физические системы защиты могут включать в себя использование видеонаблюдения, системы контроля доступа, а также физические барьеры и блокировки, чтобы предотвратить физическую порчу или кражу оборудования.

– благодаря физическим системам защиты информации можно защититься от вредоносного программного обеспечения, требующего физического взаимодействия с компьютерным оборудованием. Например, системы могут быть настроены таким образом, чтобы запрещать использование USB-устройств или CD/DVD-накопителей, которые могут служить входными точками для вирусов, троянов или другого вредоносного программного обеспечения.

**1.4** **Организационные системы защиты информации**

К организационным системам защиты информации относятся:

– политики безопасности: набор правил и рекомендаций, определяющие, как организация должна обеспечивать безопасность информации, включая политику доступа, сохранение данных и поддержание конфиденциальности.

– обучение персонала по безопасности: процесс обучения сотрудников организации основам безопасности информации, угрозам и методам защиты данных, а также о правильном использовании систем и средств безопасности.

– физическая безопасность зданий и помещений: меры и процедуры, обеспечивающие безопасность физической инфраструктуры организации, включая контроль доступа к зданиям, видеонаблюдение и управление ключами.

– регулярные проверки безопасности: процесс аудита и проверки систем безопасности организации для выявления уязвимостей и слабых мест, а также для обеспечения соответствия с внутренними и внешними стандартами безопасности.

Организационные системы защиты информации относятся к комплексу мер, процедур и технологий, которые применяются для обеспечения безопасности и конфиденциальности информации в организации. Они включают в себя разработку политики безопасности информации, определение ролей и обязанностей персонала, реализацию физических, технических и организационных мер для защиты информации, а также контроль и аудит систем защиты информации.

Организационные системы защиты информации являются важным элементом в современном бизнес-мире, где потенциальные киберугрозы становятся все более продвинутыми и опасными. Эти системы предоставляют ряд преимуществ, которые делают их неотъемлемой частью деятельности любой организации.

Во-первых, организационные системы защиты информации обладают гибкостью. Они позволяют гибко настраивать и адаптировать меры безопасности под конкретные нужды организации. Каждая компания имеет свою уникальную структуру и потребности, и организационные системы защиты информации дают возможность создать индивидуальное решение, оптимально подходящее для конкретной ситуации.

Во-вторых, организационные системы защиты информации универсальны. Они могут быть применены в любой организации, независимо от ее размера, типа или отрасли. Будь то большая мультинациональная компания или небольшая стартап-компания, организационные системы защиты информации помогут обеспечить безопасность и защиту данных.

Третье преимущество организационных систем защиты информации - минимизация рисков. Они помогают организациям уменьшить риск возникновения угроз и инцидентов безопасности, таких как потеря данных или несанкционированный доступ к информации. Это особенно важно в нашей цифровой эпохе, когда информация становится все более уязвимой для атаки.  
Четвертый плюс организационных систем защиты информации - управление доступом. Они позволяют организации управлять доступом к информации, предотвращая несанкционированный доступ к конфиденциальной или чувствительной информации. Это помогает защитить данные организации и сохранить их неприкосновенность.

Пятый плюс - соблюдение законодательства. Организационные системы защиты информации помогают организациям соблюдать требования законодательства относительно защиты информации и персональных данных. Это важно для установления доверия клиентов и партнеров, а также для избежания возможных юридических проблем и штрафов.

**1.5** **Социальные системы защиты информации**

Для социальных систем защиты информации можно выделить:

– повышение осведомленности о безопасности среди пользователей: программы и мероприятия, направленные на обучение и информирование пользователей об основных принципах безопасности информации и методах защиты.

– защита от социальной инженерии: меры, направленные на защиту от манипуляций и обманных уловок, используемых злоумышленниками для получения несанкционированного доступа или конфиденциальной информации.

– политики конфиденциальности и защиты личных данных: политики и процедуры, разработанные для обеспечения конфиденциальности и защиты личных данных пользователей и клиентов.

– обработка и регистрация инцидентов безопасности: процессы, связанные с быстрым реагированием на инциденты безопасности, их регистрацией и анализом, а также восстановлением после атак или нарушений безопасности.

Социальными системами защиты информации являются комплексы мер и методов, направленных на обеспечение безопасности информации в социальной сфере. Основной целью таких систем является предотвращение несанкционированного доступа, утечки или уничтожения конфиденциальной информации, а также обеспечение конфиденциальности, целостности и доступности информации в социальных организациях или органах власти.

Социальные системы защиты информации имеют несколько преимуществ, которые способствуют улучшению безопасности и защите пользователей от различных видов кибератак. Во-первых, такие системы позволяют обнаруживать и предотвращать угрозы информационной безопасности, что позволяет оперативно реагировать на них. Это помогает восстановить нормальную работу и защитить данные от возможных повреждений или утечек.

Во-вторых, социальные системы защиты информации вовлекают широкую аудиторию в процесс обеспечения безопасности. Они поощряют людей делиться информацией о потенциальных угрозах и вирусах, что способствует общественному сотрудничеству и более эффективному предотвращению кибератак.

Третье преимущество социальных систем защиты информации - возможность сохранения конфиденциальности. Такие системы позволяют защитить персональные данные и конфиденциальную информацию пользователей, предотвращая ее утечку или неправомерный доступ. Это особенно важно в наше время, когда все больше информации онлайн и растет риск ее утраты или злоупотребления.

**2 Недостатки систем защиты информации**

**2.1 Недостатки программных систем защиты информации**

Программные системы защиты информации имеют и свои минусы. Для начала, их внедрение и поддержка могут быть сложными. Для успешной реализации таких систем требуются определенные знания и навыки. Кроме того, они могут потребовать значительных инвестиций в виде приобретения и обновления программного обеспечения, обучения персонала и других ресурсов.

Также следует отметить, что программные системы защиты информации могут иметь свои собственные уязвимости, которые могут быть использованы злоумышленниками. Поэтому необходимо регулярно обновлять системы безопасности и следить за последними тенденциями и угрозами в сфере информационной безопасности.

В целом, программные системы защиты информации предлагают множество преимуществ в обеспечении безопасности данных организации. Однако, их эффективность зависит от правильной реализации и поддержки, а также от учета собственных уязвимостей. Организации должны уделять особое внимание и усилия для обеспечения высокого уровня информационной безопасности.

**2.2 Недостатки аппаратных систем защиты информации**

У аппаратных систем защиты информации есть и свои недостатки.

Прежде всего, высокая стоимость является одним из них. Аппаратные системы защиты информации часто требуют значительных финансовых вложений, что может быть финансово непозволительным особенно для небольших и средних предприятий. Приобретение и поддержка таких систем может значительно увеличивать расходы организаций.

Второй недостаток аппаратных систем — ограниченная гибкость. По сравнению с программными решениями они могут быть менее гибкими и требовать дополнительных затрат для настройки и модификации системы под конкретные потребности организации.

Третий недостаток связан с ограничениями в масштабируемости. Аппаратные системы могут иметь ограничения в возможности масштабирования, что может ограничивать их применение в организациях с высокими потребностями в безопасности и большим объемом данных. Предприятиям, которые планируют значительное расширение своей деятельности, может потребоваться переход на более масштабируемые решения.

Наконец, внедрение и обслуживание аппаратных систем может быть сложным процессом, требующим высокой квалификации специалистов. Установка, настройка, обновление и обслуживание таких систем требует команды экспертов, что может привести к дополнительным расходам и сложностям для организаций.

В целом, аппаратные системы защиты информации являются эффективными средствами обеспечения безопасности данных, но их применение и внедрение требуют тщательного обдумывания, учета своих возможностей и ограничений, а также финансовых возможностей организации.

**2.3 Недостатки физических систем защиты информации**

Минусы физических систем защиты информации:

– физические системы защиты информации требуют дополнительных инвестиций в оборудование и установку, что может быть затратным. Организации должны выделить средства на приобретение и настройку необходимых систем, а также на обучение персонала использованию этих систем.

– физические системы защиты могут быть неэффективными в борьбе с угрозами, связанными с внутренними угрозами. Если злонамеренное действие исходит от человека, имеющего доступ к системе, физические барьеры не смогут справиться с этой угрозой. Необходимо уделить внимание внутренней безопасности и контролю доступа к данным с помощью дополнительных мер безопасности.

– физические системы защиты информации могут создавать сложности и неудобства для пользователей системы, так как включают в себя дополнительные процедуры и аутентификацию. Например, чтобы получить доступ к защищенным помещениям или использовать определенное оборудование, пользователи могут быть обязаны проходить процедуру проверки личности или использовать специальные идентификаторы. Это может занять время и неудобно для пользователей, особенно если они часто перемещаются внутри здания или имеют ограниченные возможности доступа.

**2.4 Недостатки организационных систем защиты информации**

Несмотря на все эти преимущества, организационные системы защиты информации имеют и некоторые недостатки.

Во-первых, важно постоянно обновлять эти системы и модернизировать их, чтобы сохранять их эффективность в условиях быстро меняющейся киберугрозы. Технологии и методы атаки постоянно развиваются, поэтому необходимо быть в курсе последних тенденций и обновлять системы соответствующим образом.

Во-вторых, организационные системы защиты информации могут быть скомпрометированы из-за ошибок человека. Неправильная конфигурация или неправильное использование безопасных методов могут создать уязвимости, которые будут использованы злоумышленниками. Поэтому важно обучать персонал и осуществлять постоянный контроль, чтобы избежать таких ошибок.

Третий недостаток - затраты. Внедрение и поддержка организационных систем защиты информации требуют значительных инвестиций. Необходимо провести обучение персонала, разработать политики и процедуры, приобрести и обновить технические средства. Это может быть дорогим и трудоемким процессом для некоторых организаций.

Четвертый недостаток - сложность. Организационные системы защиты информации могут быть сложными в реализации и управлении, особенно для небольших организаций без специализированного ИТ-персонала. Это может создавать дополнительные вызовы и требовать дополнительных усилий и ресурсов.

Последний недостаток - неполное покрытие. Организационные системы защиты информации могут не обеспечить полной защиты от всех видов киберугроз, особенно от новых и продвинутых угроз, которые могут быть сложными для обнаружения и предотвращения. Это означает, что наряду с организационными системами защиты информации, также необходимы другие слои и средства защиты, чтобы обеспечить полную безопасность данных и информации.

**2.5 Недостатки социальных систем защиты информации**

Социальные системы защиты информации имеют и некоторые недостатки.

Во-первых, некоторые пользователи могут не осознавать риски информационной безопасности и не принимать необходимые меры для защиты своей информации. Это может создавать риски как для самих пользователей, так и для окружающих.

Во-вторых, социальные системы защиты информации могут иногда срабатывать на ложные сигналы, что может вызывать неудобства для пользователей и снижать доверие к таким системам. Ложные срабатывания могут быть вызваны неправильным анализом данных или некорректной интерпретацией сигналов, что может создавать напряжение между пользователями и системой защиты.

Также некоторые меры защиты информации, реализуемые в социальных системах, могут быть восприняты как нарушение приватности, так как требуют сбора и анализа персональных данных пользователей. Это может вызывать определенное недоверие со стороны пользователей и повышать уровень тревоги относительно защиты их личных данных.

Кроме того, эффективность социальных систем защиты информации зависит от активной вовлеченности пользователей. Если пользователи не соблюдают необходимые меры безопасности или не проявляют достаточной осторожности в обращении с информацией, то эффективность таких систем может снижаться. Зависимость от вовлеченности пользователей может стать проблематичной в случае, если люди не осознают значимость мер безопасности или не уделяют этому достаточного внимания.

В целом, социальные системы защиты информации имеют ряд преимуществ, но их эффективность может быть ограничена из-за неполного понимания угроз, возможных ложных срабатываний, нарушения приватности и зависимости от вовлеченности пользователей. Чтобы достичь наибольшей эффективности защиты информации, необходимо совмещать различные подходы и регулярно обновлять системы, учитывая изменения в технологиях и угрозах информационной безопасности.

**3 Способы и методы минимизации и устранения недостатков систем защиты информации**

**3.1 Минимизация расходов**

Основные пути решения проблем для устранения или предотвращения излишка расходов сосредоточены на минимизации расходов:

– анализ рисков и приоритезация: оцените риски, связанные с информационной безопасностью, и определите, какие из них являются наиболее критическими для вашего предприятия. Сфокусируйтесь на решении этих проблем, чтобы использовать ресурсы более эффективно.

– разработка эффективной политики безопасности: создайте политику безопасности, которая устанавливает четкие правила и рекомендации для сотрудников по обеспечению безопасности информации. Это поможет предотвратить инциденты и снизить риски без необходимости дорогостоящих систем безопасности.

– обучение сотрудников: проводите обучения и тренинги для сотрудников по безопасности информации. Чем лучше они понимают угрозы и связанные с ними меры предосторожности, тем меньше вероятность возникновения инцидентов. Обучение также может помочь сократить необходимость в дорогих системах защиты, так как сотрудники будут более ответственны в обращении с информацией.

– используйте открытый и бесплатный софт: воспользуйтесь открытым и бесплатным программным обеспечением для систем защиты информационной безопасности, вместо покупки коммерческих продуктов. В интернете можно найти множество открытых и бесплатных программ, которые могут решить большинство базовых задач по безопасности.

– аутсорсинг: рассмотрите возможность аутсорсинга некоторых функций в области безопасности информации. Например, можно передать управление и обслуживание системы безопасности компании-специалисту, что может быть более эффективным и дешевым в долгосрочной перспективе.

– регулярное обновление и совершенствование: постоянно совершенствуйте свои системы безопасности и обновляйте их, чтобы они оставались эффективными в борьбе с новыми угрозами. Таким образом, можно уменьшить риски и снизить необходимость в дорогостоящих улучшениях.

**3.2 Комплексный подход**

Максимальная безопасность предприятия при использовании различных систем информационной безопасности требует применения комплексного подхода.

Вот несколько ключевых шагов, которые могут помочь в обеспечении безопасности:

– разработка стратегии информационной безопасности: Разработайте план, который включает в себя политики, процедуры и практики безопасности, а также установите ясные роли и ответственности для сотрудников.

– установка многоуровневой защиты: Используйте различные системы безопасности, такие как фаерволы, антивирусы, защиту от вторжений, системы обнаружения и предотвращения утечек данных и другие инструменты, чтобы максимально защитить сеть предприятия.

– организация резервного копирования данных: регулярно создавайте резервные копии всех важных данных предприятия и храните их в безопасном месте. Это поможет минимизировать потери данных в случае взлома или сбоя системы.

– аудит безопасности: проводите регулярные аудиты безопасности, чтобы выявить слабые места и потенциальные уязвимости. Это позволит быстро реагировать на угрозы и принимать соответствующие меры.  
– Разработка кризисного плана: Создайте кризисный план информационной безопасности, чтобы на случай кибератак или других аварийных ситуаций были четко определены действия и ответственности.

– мониторинг активности: Используйте системы мониторинга, чтобы отслеживать и регистрировать активность в сети предприятия. Это позволит выявить необычную или подозрительную активность и принять меры по ее предотвращению.

– сотрудничество с профессионалами безопасности: если возникают сложности или требуются дополнительные меры безопасности, обратитесь за помощью к экспертам в области информационной безопасности.

**Заключение**

В ходе выполнения данной работы по получению профессиональных умений и опыта практической деятельности на базе ДВФУ были решены следующие задачи:

– осуществлено ознакомление с классификацией систем защиты информации предприятий;

– выявлены наиболее распространённые среди предприятий системы защиты информации;

– изучены недостатки данных систем защиты информации и существующие методы устранения и ограничения недостатков систем защиты информации;

– разработан перечень наиболее эффективных мероприятий по устранению и ограничению недостатков.

Таким образом, выполнение проделанной работы по системам защиты информации предприятий значительно расширило наши знания и навыки. Мы ознакомились с различными подходами к защите информации, идентифицировали наиболее распространенные системы защиты и изучили способы устранения и ограничения их недостатков. Разработанный перечень мероприятий поможет нам как будущим специалистам в области информационной безопасности повысить эффективность системы защиты на предприятиях.

**Список использованных источников**

1. Музалевский, Ф. А. Проблемы защиты информации на предприятии [Электронный ресурс] / Ф. А. Музалевский. – Электрон. дан. – Режим доступа: <https://rtmtech.ru/articles/problemy-zashhity-informatsii-na-predpriyatii/>.
2. Ищейнов, В. Я. Системы защиты информации [Электронный ресурс] / В. Я. Ищейнов. – Электрон. дан. – Режим доступа: <https://www.top-personal.ru/officeworkissue.html?578#:~:text=%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%20%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8%20%E2%80%94%20%D1%81%D0%BE%D0%B2%D0%BE%D0%BA%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C%20%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D0%BE%D0%B2,%D0%BD%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D1%8B%D0%BC%D0%B8%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B0%D0%BC%D0%B8%20%D0%BF%D0%BE%20%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8>.
3. Примеры типовых систем защиты информации [Электронный ресурс] – Электрон. дан. – Режим доступа: <https://ib.iitrust.ru/systemi-zashiti-informatsii/>.
4. Техническая защита информации на предприятии [Электронный ресурс] – Электрон. дан. – Режим доступа: <https://searchinform.ru/services/outsource-ib/zaschita-informatsii/tekhnicheskaya/tekhnicheskaya-na-predpriyatii/>.
5. Комплексная система защиты информации предприятия [Электронный ресурс] – Электрон. дан. – Режим доступа: <https://vsbdo.com/zashita_informazii>.
6. Информационная безопасность предприятия: ключевые угрозы и средства защиты [Электронный ресурс] – Электрон. дан. – Режим доступа: <https://www.smart-soft.ru/blog/informatsionnaja-bezopasnost/>.