УДК 004.056.5

С.В. Корякин, srgkoryakin1@gmail.com
1Институт информационных технологий КГТУ им. И.Раззакова
2Институт машиноведения автоматики и геомеханики НАН КР
С.Н. Верзунов,
Институт машиноведения автоматики и геомеханики НАН КР
П.Л. Вейс, veis_p@iuca.kg
Международный университет в центральной Азии
А.К. Оруналиева,
Институт информационных технологий КГТУ им. И. Раззакова

АНАЛИТИЧЕСКИЙ ОБЗОР МЕТОДОВ И СПОСОБОВ РЕАЛИЗАЦИИ СИСТЕМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИТИИ

Аннотация. *В статье приводится анализ методов и технологий, применяемых для построения систем защиты персональных данных (ТЗПД) на предприятиях. Рассматриваются и предлагаются различные подходы к их реализации. Особое внимание уделено как правовому регулированию в Кыргызской Республике, так и международным стандартам. Приведены примеры эффективных решений, применяемых для защиты информации, а также обсуждаются стратегии управления рисками, связанные с утечкой и несанкционированным доступом к данным.*

Ключевые слова: *защита данных, персональные данные, информационная безопасность, инструменты безопасности, технологии защиты, шифрование, системы IDS/IPS, управление доступом (IAM), антивирусное ПО, файрволлы, многофакторная аутентификация (MFA), резервное копирование данных, DLP-системы, SIEM-системы, управление инцидентами безопасности, аудит доступа, обучение сотрудников, предотвращение утечек данных, киберугрозы, защита конфиденциальной информации.*

Защита персональных данных, обрабатываемых организациями, в настоящее время является одной из наиболее актуальных проблем в сфере информационной безопасности и кибер-безопасности. Увеличение объемов данных, а также частота инцидентов, связанных с утечками, создают необходимость разработки комплексных систем защиты, которые соответствуют не только требованиям бизнеса, но и законодательным нормам. В Кыргызской Республике данный вопрос регулируется Законом «О персональных данных» № 58 от 14 апреля 2008 года [1], который устанавливает обязательства организаций по защите персональных данных, а также штрафные санкции за несоблюдение этих обязательств. Следует отметить, что в глобальном контексте важную роль играет GDPR — нормативно-правовой акт Европейского Союза, касающийся обработки персональных данных [2].

Целью проводимого в данной работе исследования является глубокий анализ современных подходов к созданию систем защиты персональных данных в корпоративной среде, а также оценка их эффективности с точки зрения минимизации возможных рисков. Именно по этой причине при построении ПЗПД предлагается выделить следующе основные аспекты которые наиболее полно способствуют реализации функциональных возможностей и эффективности разрабатываемых ПЗГД: Правовые основы и регуляторные требования, классификация подходов к защите данных, технические решения для защиты данных, управление рисками и предотвращение утечек данных, Адаптивные меры защиты в условиях изменяющихся угроз.

1. Правовые основы и регуляторные требования

Первостепенным аспектом в вопросе защиты данных на предприятиях является выполнение законодательных и нормативных требований. В Кыргызской Республике, как уже было упомянуто, нормативной базой для защиты персональных данных выступает Закон № 58 «О персональных данных» [1], который определяет обязательства субъектов данных и операторов. Этот закон устанавливает принципы, по которым компании обязаны обрабатывать и хранить персональные данные, включая необходимость обеспечения их безопасности.

Следует подчеркнуть, что данные нормы предполагают внедрение комплексных мер защиты, направленных на предотвращение как внешних, так и внутренних угроз. Эти меры охватывают как технические аспекты защиты данных, так и организационные мероприятия, обеспечивающие их соблюдение [3].

2. Классификация подходов к защите данных

Существующие подходы к защите персональных данных можно условно разделить на три большие категории: организационные, технические и физические меры. Каждая из них нацелена на устранение или минимизацию различных типов угроз.

Организационные меры включают разработку внутренних политик и процедур, регламентирующих порядок обработки данных и поведение сотрудников при работе с ними. Обучение сотрудников и контроль за выполнением установленных правил играют ключевую роль в снижении рисков, связанных с человеческим фактором [4].

Технические меры реализуются через использование специализированного программного обеспечения и аппаратных решений. Например, одним из основных методов защиты данных является шифрование, которое делает информацию недоступной для третьих лиц в случае утечки. Используются как симметричные (AES), так и асимметричные алгоритмы шифрования (RSA) [5]. Также активно применяются технологии многофакторной аутентификации (2FA), что существенно снижает риск несанкционированного доступа [6].

Физические меры направлены на защиту инфраструктуры и оборудования. К ним можно отнести контроль доступа к серверным комнатам, использование биометрических систем и видеонаблюдение. Эти методы обеспечивают защиту от физических угроз, таких как кража оборудования или саботаж [7].

3. Технические решения для защиты данных

Одним из ключевых элементов любой системы защиты является шифрование данных, которое гарантирует, что даже при утечке информации злоумышленники не смогут её расшифровать. В современных условиях симметричное шифрование (например, алгоритм AES) широко используется для защиты больших объемов данных, тогда как асимметричное шифрование (RSA, ECC) применяется для более специфичных задач, таких как защита ключей и аутентификация [5].

Кроме шифрования, важную роль в защите персональных данных большую роль играет использование систем мониторинга и анализа событий информационной и кибербезопасности так называемых SIEM-систем. Такие системы позволяют в реальном времени отслеживать инциденты, проводить анализ сетевого трафика и оперативно реагировать на возможные угрозы [8]. SIEM-инструменты дают возможность собирать и анализировать данные о событиях, происходящих в информационной системе, что позволяет предотвратить потенциальные атаки до их реализации.

Особое внимание следует уделить многофакторной аутентификации (MFA), которая позволяет повысить уровень безопасности, требуя от пользователей предоставления нескольких доказательств их личности. Это может быть сочетание пароля, физического токена и биометрических данных, что значительно усложняет задачу злоумышленникам [9].

4. Управление рисками и предотвращение утечек данных

Для обеспечения должного уровня безопасности важно не только применять технические и организационные меры, но и грамотно управлять рисками. Оценка рисков позволяет выявить наиболее уязвимые точки в системе защиты и разработать адекватные меры для их минимизации [10]. В частности, применение методик управления рисками,

основанных на стандартах ISO/IEC 27001, позволяет структурировать процессы и создать эффективную систему управления информационной безопасностью (СУИБ) [11].

Кроме того, одним из важнейших инструментов для предотвращения утечек данных являются системы DLP (Data Loss Prevention). Эти решения позволяют контролировать перемещение данных внутри организации, предотвращать их утечку за её пределы и блокировать несанкционированные действия пользователей. DLP-системы обеспечивают фильтрацию трафика, контроль за копированием данных и анализ подозрительных активностей [12].

5. Адаптивные меры защиты в условиях изменяющихся угроз

Современная киберсреда постоянно эволюционирует, что требует от предприятий адаптации к новым типам угроз. С каждым годом растет количество кибератак, направленных на получение персональных данных (ПД). В этой связи важным становится внедрение технологий, основанных на искусственном интеллекте и машинном обучении, которые позволяют предсказывать и эффективно реагировать на новые угрозы [13].

Применение ИИ и машинного обучения в области информационной безопасности и кибер-безопасности открывает новые горизонты для построения гибких и устойчивых систем защиты. Эти технологии способны анализировать огромные объемы данных в режиме реального времени, выявлять аномалии и самостоятельно принимать решения о блокировке подозрительной активности [14].

Следует отметить, что на сегодняшний день в условиях стремительного развития информационных технологий, а также с учетом всеобщей цифровизации объектов критической инфраструктуры организаций наблюдается увеличение объема обрабатываемых данных внутри киберфизических систем. В связи с этим защита персональных данных становится одной из ключевых задач для предприятий. Угроза утечек и несанкционированного доступа к конфиденциальной информации требует внедрения комплексных мер безопасности. В Кыргызской Республике защита персональных данных регулируется рядом законодательных актов, таких как Закон "О персональных данных", «Закон о кибербезопасности» и Уголовный кодекс Кыргызской Республики, предусматривающий ответственность за нарушение правил обработки и защиты персональных данных.

Считается что, для создания систем защиты ПД используются следующие современные инструменты и технологии, которые предлагается разделить на основные - базовые и дополнительные – опциональные.

К основным - базовым системам предлагается отнести следующие: системы предотвращения вторжений, шифрование данных, системы управления идентификацией и доступом (IAM), антивирусное ПО и антималварные решения, файрволлы (межсетевые экраны), системы резервного копирования и восстановления данных.

Дополнительными или опциональными предлагается называть: многофакторная аутентификация (MFA), DLP-системы (Data Loss Prevention), SIEM-системы (Security Information and Event Management), учет и аудит доступа к данным, управление инцидентами безопасности.

1. Системы предотвращения вторжений (IDS/IPS)

Эти системы отслеживают сетевой трафик и активность на предмет подозрительной деятельности и попыток вторжений. IDS (Intrusion Detection Systems) обнаруживают и сообщают о подозрительных действиях, в то время как IPS (Intrusion Prevention Systems) не только обнаруживают, но и предотвращают такие действия (рис. 1).

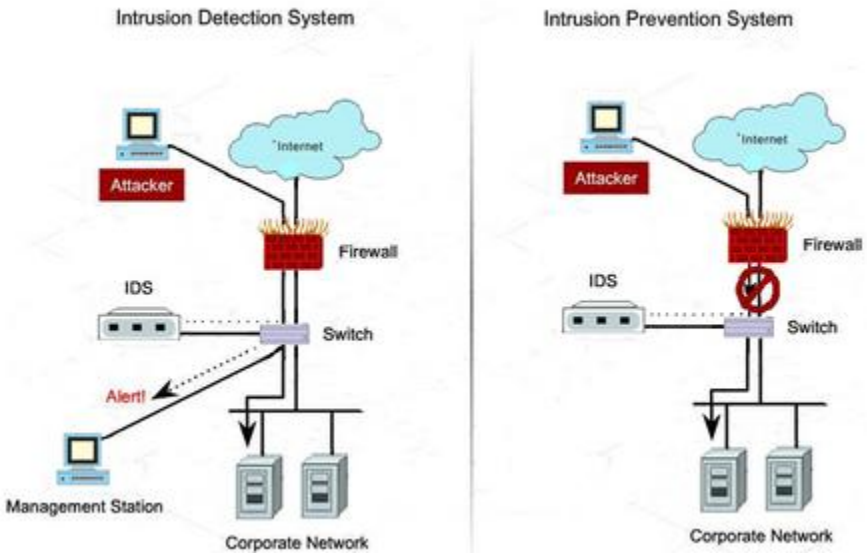

Рисунок 1. Обобщенная структурная схема IDS/IPS

В качестве самых распространённых в использовании из существующих IDS/IPS систем в настоящее время считаются: Snort – популярная IDS с открытым исходным кодом, Cisco Firepower – комплексное решение, включающее IDS и IPS[15]. Кроме того, следует отметить, что существует очень большое количество IDS и IPS решений, которые широко используются специалистами по кибербезопасности, при этом выбор того или иного решения зависит от личных предпочтений специалиста, а также требований стандартов и нормативных документов, используемых при реализации систем защиты персональных данных.

2. Шифрование данных

Шифрование данных обеспечивает защиту информации путем преобразования её в зашифрованный текст, который может быть расшифрован только при наличии соответствующего ключа. Существует несколько типов шифрования, включая симметричное и асимметричное (рис. 2).

Примеры решений для шифрования:

- AES (Advanced Encryption Standard) – стандарт симметричного шифрования.
- RSA – алгоритм асимметричного шифрования, широко используемый для защиты данных[16].

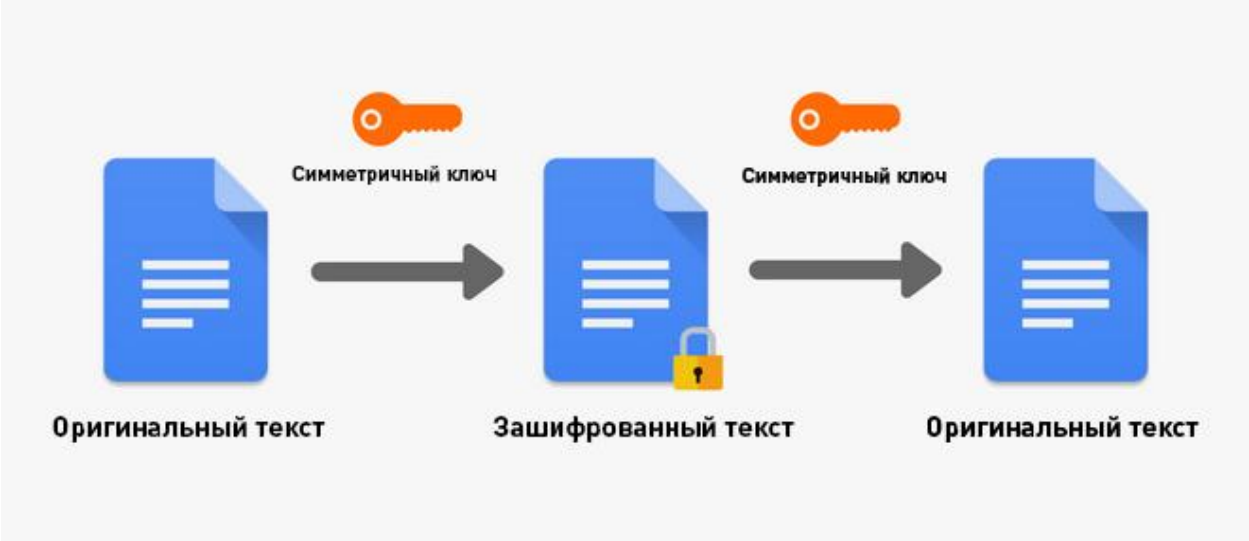

Рисунок 2: Обобщенный вариант процесса шифрования данных

3. Системы управления идентификацией и доступом (IAM)

IAM (Identity and Access Management) позволяет контролировать доступ сотрудников к информационным ресурсам на основе их ролей и полномочий. Эти системы включают в себя управление учетными записями пользователей, аутентификацию и авторизацию (рис.3).

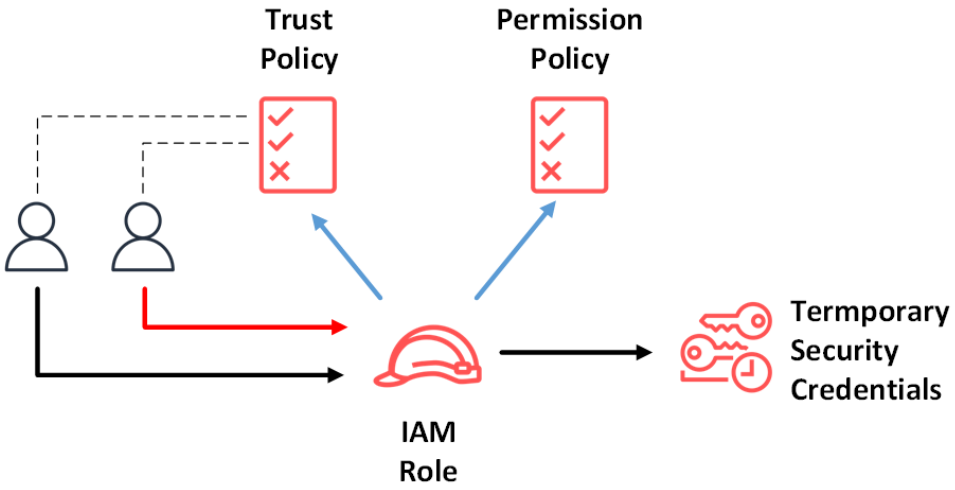

Рисунок 3: Обобщенная схема работы IAM

Из наиболее используемых IAM систем предлагается выделить: Microsoft Azure Active Directory – облачная служба управления идентификацией, Okta – платформа управления идентификацией и доступом[17].

4. Антивирусное ПО и антималварные решения

Антивирусные программы и антималварные решения предназначены для обнаружения, предотвращения и удаления вредоносных программ. Они работают на основе сигнатур и методов эвристического анализа, применяемого в СЗПД для защиты от известных и новых киберугроз. Наиболее известными примерами антивирусного ПО являются**:** Kaspersky Antivirus – антивирусное ПО, известное своей высокой эффективностью., Norton Security – комплексное решение для защиты от вредоносного ПО.

5. файрволлы (межсетевые экраны).

файрволлы ограничивают несанкционированный доступ к сетям предприятия, фильтруя входящий и исходящий трафик на основе заданных правил безопасности. Они могут быть аппаратными или программными.

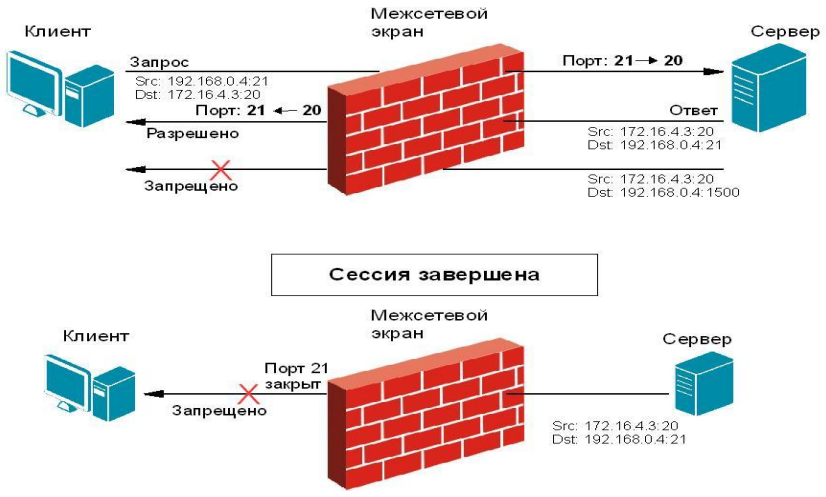

Рисунок 4: Принцип работы межсетевого экрана

Следует выделить такие решения как Cisco ASA – аппаратный файрволл., pfSense – программный файрволл с открытым исходным кодом, которые получили очень широкое применение в СЗПД[15.18].

6. Системы резервного копирования и восстановления данных

Считается что резервное копирование данных обеспечивает их сохранность в случае сбоев или атак. Эти системы позволяют восстанавливать данные из резервных копий, хранящихся на удаленных серверах или внешних носителях (рис. 5).

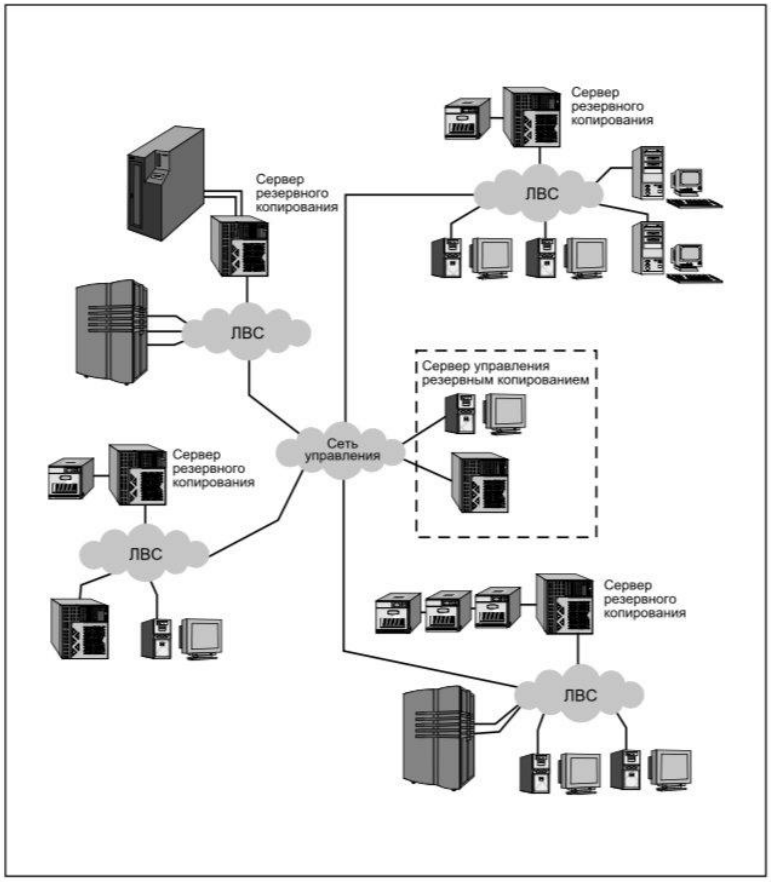

Рисунок 5. Обобщенная структурная схема системы резервного копирования

Из наиболее распространенных вариантов систем для резервного копирования данных выделяют: Veeam Backup & Replication – решение для резервного копирования и восстановления данных и Acronis Backup – программное обеспечение для создания резервных копий и восстановления данных.

Дополнительные технологии и инструменты информационной безопасности

1. Многофакторная аутентификация (MFA).

Многофакторная аутентификация добавляет дополнительный уровень безопасности, требуя от пользователей подтверждать свою личность несколькими способами, такими как пароли, отпечатки пальцев или SMS-коды.

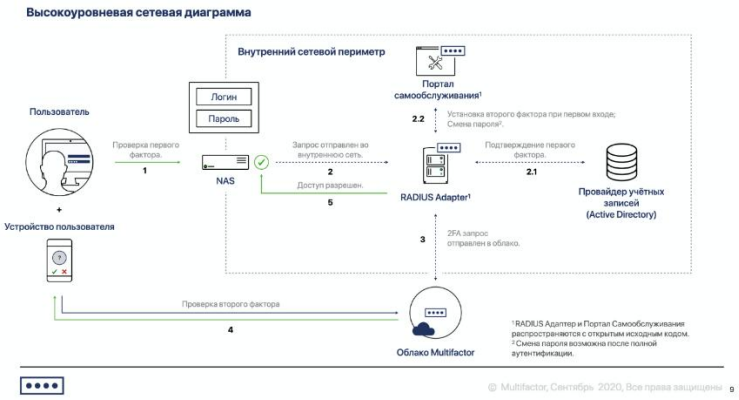

Рисунок 6: Принцип работы системы многофакторной аутентификаций

Примеры решений для MFA Google Authenticator – приложение для создания одноразовых паролей и Duo Security – решение для многофакторной аутентификации[19].

2. DLP-системы (Data Loss Prevention)

Системы предотвращения утечек данных (DLP) предназначены для обнаружения и предотвращения несанкционированной передачи конфиденциальной информации за пределы организации.

Примеры DLP решений

- Symantec Data Loss Prevention – комплексное решение для защиты данных.
- Digital Guardian – платформа для предотвращения утечек данных.

3. SIEM-системы (Security Information and Event Management)

Системы управления информацией и событиями безопасности (SIEM) собирают, анализируют и предоставляют отчеты о событиях безопасности в реальном времени.

Наиболее распространенными примерами SIEM систем являются: Splunk – платформа для мониторинга и анализа данных, IBM QRadar – решение для управления информацией и событиями безопасности и др..

4. Обучение и повышение осведомленности сотрудников

Одним из ключевых аспектов защиты персональных данных является обучение сотрудников принципам информационной безопасности. Регулярные тренинги и курсы повышают осведомленность персонала о потенциальных угрозах и мерах защиты.

5. Учет и аудит доступа к данным

Для обеспечения безопасности персональных данных необходимо регулярно проводить учет и аудит доступа к данным. Это позволяет отслеживать, кто и когда имел доступ к конфиденциальной информации, и выявлять возможные нарушения.

6. Управление инцидентами безопасности

Эффективное управление инцидентами безопасности включает в себя разработку процедур и планов действий на случай нарушения безопасности данных. Это позволяет минимизировать последствия инцидентов и быстро восстанавливать нормальную работу системы.

В таблице 1 представлен сравнительный анализ характеристик современных технологий и инструментов при создании СЗПД на предприятии[20].

Таблица 1. сравнительный анализ характеристик современных технологий и инструментов при создании СЗПД на предприятии

Технология/Метод	Преимущества	Недостатки
Системы обнаружения и предотвращения вторжений	- Высокий уровень обнаружения угроз	- Высокая стоимость

(IDS/IPS)	- Возможность автоматического реагирования на инциденты безопасности	- Возможные ложные срабатывания
Шифрование данных	- Высокий уровень защиты данных	- Затраты на вычислительные ресурсы
	- Возможность использования в различных средах	- Сложности в управлении ключами
Управление доступом к информации (IAM)	- Централизованное управление доступом	- Сложность внедрения
	- Снижение риска несанкционированного доступа	- Необходимость постоянного администрирования
Антивирусное программное обеспечение (ПО)	- Обнаружение и удаление большинства вредоносных программ	- Возможность пропуска новых угроз
		- Замедление работы системы
Файрволлы	- Эффективная защита сети	- Сложность настройки и администрирования
	- Возможность настройки правил доступа	- Не защищают от внутренних угроз
Системы резервного копирования	- Восстановление данных в случае сбоев	- Требуют значительных ресурсов для хранения
	- Защита от потерь данных	- Возможность устаревания резервных копий
Многофакторная аутентификация (MFA)	- Повышение уровня безопасности за счет дополнительных факторов аутентификации	- Увеличение времени доступа
		- Необходимость дополнительного оборудования или ПО
DLP-системы	- Защита конфиденциальной информации	- Сложность настройки и управления
	- Предотвращение утечек данных	- Высокая стоимость
SIEM-системы	- Мониторинг безопасности в реальном времени	- Высокая стоимость внедрения и эксплуатации
	- Возможность анализа и корреляции событий	- Необходимость квалифицированного персонала

Обучение и повышение осведомленности сотрудников	- Уменьшение числа инцидентов, связанных с человеческим фактором	- Необходимость регулярного проведения тренингов
	- Повышение уровня ответственности сотрудников за защиту данных	- Требование ресурсов для разработки и проведения обучающих программ
Учет и аудит доступа к данным	- Возможность быстрого выявления несанкционированного доступа	- Требует внедрения специализированного ПО
	- Учет всех действий, связанных с обработкой данных	- Необходимость в ресурсах для проведения регулярных аудитов
Управление инцидентами безопасности	- Сокращение времени реагирования на инциденты	- Необходимость постоянного обновления планов и процедур
	- Снижение ущерба от потенциальных утечек данных	- Требует квалифицированного персонала для управления инцидентами

Таким образом из проведенного анализа технологий решения и методов построения ПЗПД с целью обеспечения надежной защиты персональных данных на предприятии рекомендуется использовать комплексный подход, включающий мероприятия реализующие следующие обязательные функции ПЗПД:

- Внедрение IDS/IPS для мониторинга и защиты от сетевых атак.
- Использование шифрования данных для защиты информации как в покое, так и при передаче.
- Реализация IAM для управления доступом к информационным ресурсам на основе политики доступа.
- Установка антивирусного ПО для защиты от вредоносных программ.
- Настройка файрволлов для ограничения несанкционированного доступа к сети предприятия.
- Регулярное создание резервных копий данных и проверка их на целостность.
- Внедрение многофакторной аутентификации для повышения уровня безопасности.
- Использование DLP-систем для предотвращения утечек данных.
- Внедрение SIEM-систем для мониторинга и анализа событий безопасности в реальном времени.

На основании проведенного анализа можно сделать вывод о том, что для обеспечения эффективной защиты персональных данных на предприятиях необходимо применять комплексный подход, сочетающий технические, организационные и правовые меры. Современные технологии, такие как шифрование, многофакторная аутентификация и системы мониторинга, играют ключевую роль в предотвращении утечек данных и защите от несанкционированного доступа. Внедрение риск-ориентированных подходов и адаптация систем безопасности к новым вызовам позволит повысить устойчивость предприятий к внешним и внутренним угрозам. Следует отметить, что успешная реализация системы защиты данных невозможна без учета специфики бизнеса и постоянного мониторинга

актуальных угроз и уязвимостей. В этом контексте важную роль играет внедрение систем управления информационной безопасностью, основанных на международных стандартах, таких как ISO/IEC 27001.

Список литературы

1. Закон Кыргызской Республики «О персональных данных» от 14 апреля 2008 года № 58.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
3. Указ Президента Кыргызской Республики «О мерах по защите персональных данных» от 1 марта 2017 года.
4. Лившиц В.М., Шестаков Д.В. Информационная безопасность организаций. – М.: Юнити-Дана, 2020. – 320 с.
5. Сорокин В.А. Методы защиты информации. – СПб.: Питер, 2019. – 456 с.
6. Stallings W. Cryptography and Network Security: Principles and Practice. – Pearson, 2020. – 816 p.
7. Журавлев В.П. Защита информации в корпоративных системах. – М.: Горячая Линия – Телеком, 2019. – 384 с.
8. Williams, P. and Wills, L. Security Information and Event Management (SIEM) Implementation. – McGraw-Hill, 2018.
9. Cuppens, F., & Miege, A. Intrusion Detection Systems. – Springer, 2021. – 512 p.
10. Kizza, J.M. Guide to Computer Network Security. – Springer, 2020. – 535 p.
11. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
12. Harris S. CISSP All-in-One Exam Guide. – McGraw-Hill Education, 2019. – 1456 p.
13. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2020. – 1088 p.
14. Bishop, M. Introduction to Computer Security. – Addison-Wesley, 2020. – 786 p.
15. Бойко, В. В. (2021). Информационная безопасность. М.: Юрайт. http://www.publishing-vak.ru/file/archive-economy-2021-2/16-ershova-boiko.pdf
16. Снитко, С. А. (2020). Управление информационной безопасностью. https://rusneb.ru/catalog/000199_000009_010930271/
17. Kaufman, C., Perlman, R., & Speciner, M. (2016). Network Security: Private Communication in a Public Internet. Prentice Hall. (https://www.pearson.com/store/p/network-security-private-communication-in-a-public-internet/P100000323269
18. Symantec Corporation. (2020). Symantec Data Loss Prevention. https://cortex.marketplace.pan.dev/marketplace/details/SymantecDLP/#:~:text=Symantec%20Data%20Loss%20Prevention%20(DLP),of%20your%20sensitive%20corporate%20data
19. Cisco Systems. (2019). Cisco Firepower Next-Generation Firewall. https://www.cisco.com/c/dam/m/ru_ua/campaigns/security-hub/pdf/datasheet-c78-736661.pdf
20. Microsoft Corporation. (2021). Microsoft Azure Active Directory. https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id