Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическое задание №2**

**Тема «Разработка политики информационной безопасности бизнес-компании»**

Руководитель: Ржеутская Н. В.

Выполнил:

Студент 2 курса 1 группы ФИТ

Немкович Анастасия Вадимовна

Минск 2023

Цель: Разработать проект политики информационной безопасности бизнес-компании.

**Условие задания**

Разработать проект политики информационной безопасности бизнес-компании, оформив результаты в виде пояснительной записки. Пояснительная записка может, например, содержать следующие разделы:

1. Титульный лист;
2. Введение (обосновывается важность разработки политики информационной безопасности);
3. Описание структуры бизнес-компании (выбор компании предварительно согласовывается с преподавателем);
4. Оценка рисков;
5. Разработка мер защиты;
6. Выводы.

Электронный вариант вносится в электронную тетрадь и показывается преподавателю для предварительной проверки (объем – 10-20 страниц).

|  |  |
| --- | --- |
| 12 | Туристическая компания |

**Введение**

Под информационной безопасностью предприятия или компании понимают комплекс мер организационного и технического характера, направленных на сохранение и защиту информации и ее ключевых элементов, а также оборудование и системы, которые используются для работы с информацией, ее хранения и передачи. Этот комплекс включает технологии, стандарты и методы управления информацией, которые обеспечивают ее эффективную защиту.

Обеспечение информационной безопасности помогает защитить информацию и информационную инфраструктуру предприятия от негативных воздействий. Такие воздействия могут носить случайный или преднамеренный, внутренний или внешний характер. Результатом таких вмешательств может стать потеря важной информации, ее несанкционированное изменение или использование третьими лицами. Поэтому информационная безопасность — это важный аспект защиты бизнеса и обеспечения его непрерывности.

Проблема сохранности конфиденциальной информации и коммерческой тайны существовала и ранее. Но по мере развития электронных средств обработки и хранения данных повышается вероятность их утечки и незаконного копирования. Если ранее для кражи чертежей нового продукта нужно было физически вынести их с завода, сейчас достаточно получить доступ к серверу через электронные каналы связи или записать их на миниатюрную карту памяти.

В большинстве случаев краже подлежат следующие данные:

* Информация о реальном финансовом состоянии компании;
* Инновационные разработки научно-технических отделов;
* Регистрационные данные для доступа к защищенным серверам;
* Персональные данные работников;
* Персональные данные клиентов.

Дополнительной сложностью является то, что кража информации может негативно отразиться на компании не сразу после ее совершения, а по прошествии определенного времени. Неважные на первый взгляд данные при их обнародовании могут нанести колоссальный вред компании и уменьшить ее рыночную стоимость.

Поэтому при разработке мер по обеспечению информационной безопасности нельзя делить данные на виды. Все, что размещено в IT-инфраструктуре компании и храниться в архивах, не должно выходить за ее пределы.

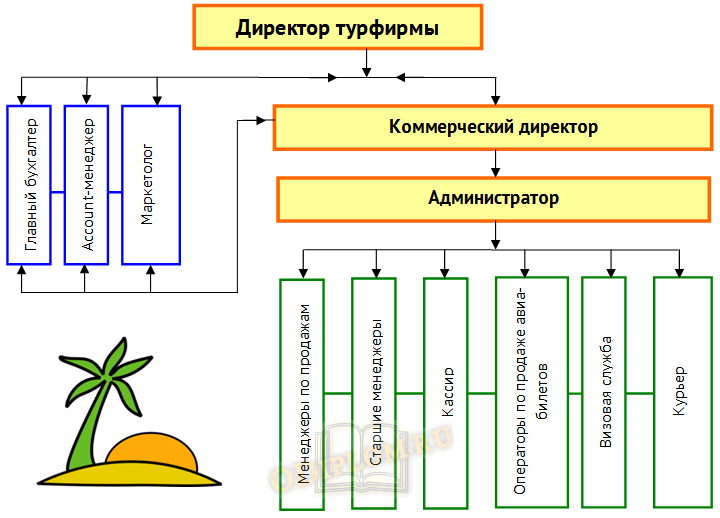
**Описание структуры бизнес-компании**

Структура туристической компании – это определенная совокупность компонентов для достижения целей компании, удовлетворения запросов потребителей и получения запланированной прибыли.

Типовой набор услуг турфирмы:

* Услуги в области туризма, организация и участие в организации и эксплуатации отелей, турбаз, мотелей, услуги по организации экскурсий, обслуживание частных и деловых поездок, культурных, гастрольных, благотворительных и других мероприятий;
* Организация туристических поездок, командировок специалистов;
* Осуществление международной туристической деятельности в ближнем и дальнем зарубежье;
* Продажа авиабилетов на внутренние и зарубежные рейсы авиакомпаний различных стран;
* Реализация путевок в здравницы и дома отдыха.

Функции турфирмы вытекают из сферы её деятельности: предоставление населению возможностей отдохнуть во время отпуска.



Пример структуры турфирмы

Согласно организационной структуре существует следующий характер связей между структурными подразделениями:

* вертикальная связь соединяет иерархические уровни в организации и существует между генеральным директором, коммерческим директором и администратором;
* горизонтальные связи – это связи между членами организации и существуют они между маркетологом, account-менеджером, главным бухгалтером, менеджерами по продажам, старшими менеджерами, кассиром, операторами по продаже авиа-билетов, визовой службой и курьером;
* функциональные связи имеют в организационной иерархии направленность снизу вверх и выступают в форме совета или рекомендации и существует между маркетологом, account-менеджером, коммерческим директором и генеральным директором;
* линейная связь, т.е. прямое руководство подчиненными в форме приказов и распоряжений, существует между генеральным директором и остальным персоналом фирмы включая коммерческого директора.

Большинство турфирм можно отнести к организациям механистического типа. Несмотря на то, что фирма имеет динамичное внешнее окружение, а специалисты обладают определенной долей свободы в принятии оперативных решений, существует жесткая иерархия власти, фирма характеризуется централизованным принятием решений на верхнем уровне управления генеральным директором и коммерческим директором.

Значительное количество турфирм являются индивидуалистскими организациями, так как сотрудники фирмы – это люди с определенными навыками, знаниями и квалификацией, которые работают в условиях свободного объединения. Также в турфирме активно используются различные мероприятия по повышению квалификации сотрудников, тренинги, обучающие программы и т.п., для стимулирования персонала применяется сложная система материальных и моральных поощрений и социальных выплат.

В соответствии с типовой организационной структурой в турфирме существует 3 уровня управления:



Уровни структуры управления в турфирме

В турфирме существует иерархическая структура управления. Она характеризуется определенной предсказуемостью поведения членов организации, как во внутреннем общении, так и при контактах с внешней средой.

Информационным центром является директор, на котором замыкаются все информационные потоки: управленческий, финансовый, материальный.

К преимуществам такой структуры турфирмы относятся:

* осуществление постоянного контроля за выполнением всех этапов работы;
* высокая квалификация персонала, профессионализм и большой опыт работы;
* комплексная работа по оказанию туристических услуг;
* индивидуальный подход к каждому клиенту;
* высокое качество оказываемых услуг;
* сотрудничество фирмы с партнерами, успешно зарекомендовавшими себя за рубежом.

**Оценка рисков**

Проблемы информационной безопасности постоянно усугубляется процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем. Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением.

Для туристической компании утечка данных может иметь серьезные последствия, так как она обрабатывает конфиденциальную информацию клиентов, бронирует путешествия и хранит данные о платежах. Давайте проведем анализ рисков по каждому этапу:

1. Идентификация ресурса и оценивание его количественных показателей:

* Ресурс: Клиентская база данных с личными данными и платежной информацией.
* Количественные показатели негативного воздействия: Утечка личных данных может привести к потере репутации, судебным и финансовым последствиям, а также штрафам в соответствии с законодательством о защите данных.

2. Оценивание угроз:

* Кибератаки: Взлом базы данных, вирусы, фишинг и мошенничество.
* Внутренние угрозы: Несанкционированный доступ сотрудников, утечка данных по недоразумению или из-за непосредственных действий сотрудников.
* Форс-мажорные события: Потеря данных из-за природных катастроф, пожаров или других чрезвычайных обстоятельств.

3. Оценивание уязвимостей:

* Недостаточную киберзащиту: Устаревшие системы безопасности, недостаточное обновление программного обеспечения.
* Несанкционированный доступ: Низкий уровень аутентификации и авторизации, слабые пароли, доступ к данным без необходимости.
* Неэффективное управление доступом: Недостаточное ограничение доступа сотрудников к конфиденциальной информации.

4. Оценивание существующих и предполагаемых средств обеспечения:

* Существующие средства включают в себя антивирусное программное обеспечение, брандмауэры и системы мониторинга безопасности.
* Предполагаемые средства могут включать в себя улучшение политики паролей, обучение сотрудников по вопросам кибербезопасности, внедрение системы обнаружения вторжений и регулярное аудирование безопасности.

Риски могут быть оценены с учетом вероятности угрозы, уязвимости и потенциальных последствий. Например, вероятность успешного кибератаки может быть низкой, но потенциальные последствия для компании могут быть катастрофическими.

На основе проведенного анализа, туристическая компания должна разработать и внедрить комплекс мер по улучшению информационной безопасности, включая улучшение политики безопасности, регулярное обновление программного обеспечения, обучение сотрудников и мониторинг активности для своей защиты от потенциальных рисков утечки данных.

Важно управлять информационной системой в целом и механизмами безопасности в особенности. Упомянутые меры безопасности должны опираться на общепринятые стандарты, быть устойчивым к сетевым угрозам, учитывать специфику отдельных сервисов.

**Разработка мер защиты**

Основой мер административного уровня, то есть мер, предпринимаемых руководством организации, является политика безопасности.

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

1) Идентификация и аутентификация субъектов доступа и объектов доступа – меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности);

2)  Управление доступом субъектов доступа к объектам доступа - меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил;

3) Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных) - меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных;

4)  Регистрация событий безопасности – меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них;

5) Антивирусная защита – меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Защита осуществляется программным, физическим, административным путем. К последнему относится:

* создание внутренних нормативно-правовых актов и подписание договоров со всеми сотрудниками о «неразглашении» и правилах использования, передачи полученной информации;
* обеспечение контроля за исполнением локальных нормативных документов;
* наличие эффективного метода аутентификации, с разграничением уровней доступа к массивам информации;
* регулярная проверка работоспособности, эффективности и своевременный апгрейд систем управления информационной безопасностью предприятия;
* постоянное резервное копирование для восстановления инфосистемы в случае сбоя, атаки или падения.

Что касается программного обеспечения, то рекомендуется внедрение специального ПО:

* Стационарный антивирусный софт. Он способен проверять компьютер на «заражение» по установленному графику или запускаться администратором, а в случае подозрительных действий отдельной программы, может уведомить об этом администратора и автоматически заблокировать ее;
* Внедрение DLP (Data Loss Prevention). Эти программы решают проблему основной угрозы информационной безопасности предприятий – утечку данных;
* Шифрование (криптография);
* Блокировка или фильтрация трафика брандмауэром, межсетевым экраном – таким образом корпоративная сеть будет отделена от глобальной, с возможностью выхода в интернет только в русле установленных ограничений;
* Использование VPN станет хорошим решением для обеспечения информационной безопасности организации с разветвленной системой филиалов, когда необходим выход в интернет или удаленное подключение к локальной сети;
* SIEM мониторинг фиксирует и сохраняет все логи системы для дальнейшего их анализа на предмет выявления несанкционированных или вредоносных действий как извне, так и изнутри;
* Фильтрация содержимого электронной почты. Специальные фильтры просматривают содержимое входящей/исходящей корреспонденции, отсекают СПАМ, зараженные вирусом письма и блокируют отсылку файлов/данных с конфиденциальной информацией.

На базе перечисленных средств защиты информации строится первый уровень подсистем информационной безопасности. На втором этапе развития системы отдельные рабочие станции объединяют в локальные сети, устанавливают выделенные сервера и организуют выход из локальной сети в интернет. На данном этапе используются средства защиты информации – уровня защиты локальной сети:

* средства безопасности сетевых операционных систем;
* средства разграничения доступа к разделяемым ресурсам;
* средства защиты домена локальной сети;
* сервера аутентификации пользователей;
* межсетевые экранные прокси-сервера;
* средства обнаружения атак и уязвимостей защиты локальной сети.

Физические меры защиты – это разного рода механические, электро- и электронно-механические устройства, сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам информационной системы и охраняемой информации. В перечень физических способов защиты информации входят: организация пропускного режима; организация учёта, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией; распределение реквизитов разграничения доступа; организация скрытого контроля за деятельностью пользователей и обслуживающего персонала информационной системы; мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях аппаратного и программного обеспечения.

Организационные меры системы защиты персональных данных туристической компании включают в себя:

* физическую защиту помещений информационной системы персональных данных предприятия;
* организационно-распорядительную документацию (положения об обработке персональных данных, распоряжение о контролируемой зоне);
* инструктивно-методическую документацию (инструкция пользователям, инструкция администратору безопасности информации, инструкция по резервированию и восстановлению персональных данных, журнал учета цифровых носителей информации).

С целью предотвращения утечки персональных данных о клиентах туркомпании работникам рекомендуется придерживаться следующих правил информационной политики безопасности:

* Не пользоваться публичными Wi-Fi сетями и точками доступа, а в случае такой необходимости использовать VPN соединение.
* Использовать только сложные пароли: они должны быть не менее 12 знаков длиной, не состоять из словарных слов, содержать спецсимволы и цифры.
* Пароли должны быть уникальными: не использовать один и тот же пароль для всех рабочих ресурсов.
* Пароли должны быть секретными: не записывать пароль на бумаге и не храните около рабочего места; не вписывать их в файлы и не делиться ими с коллегами.
* Если сервис позволяет включить двухфакторную аутентификацию (к примеру, SMS), нужно включить ее.
* Запрещается самостоятельно осуществлять настройку СКЗИ (средство криптографической защиты информации), вносить изменения в конфигурационные файлы средств защиты информации, предоставленных в рамках оказания услуг, отключать или переподключать СКЗИ;
* Работникам запрещается устанавливать стороннее ПО, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию;
* Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами туристической компании;
* Работники компании должны быть проинформированы об угрозах нарушения режима безопасности и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, которые нарушили принятые политику и процедуры безопасности.
* Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационной системы персональных данных, которые могут повлечь за собой угрозы безопасности, а также о выявленных ими событиях, затрагивающих безопасность, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности.

Права и обязанности субъектов компании должны быть регламентированы документами: отдельными положениями (инструкциями) по эксплуатации на каждую информационную систему компании; договорными отношениями при оказании услуг и в ходе технической поддержки; должностными инструкциями сотрудников.

Необходимо внедрение следующих способов разграничения доступа субъектов к объектам туристической компании:

1. Субъектам информационных отношений предоставляется объективно необходимый для них уровень доступа к объектам компании: специалистам компании предоставляется доступ к объектам в соответствии с их полномочиями, определенными в должностных инструкциях; сотрудникам (работникам) в рамках выполнения своих должностных обязанностей; должностным лицам организаций, поставляющих ПО и СКЗИ (средств криптографической защиты информации), а также осуществляющих их гарантийное и сервисное обслуживание и жизнеобеспечение в рамках договорных отношений на осуществление ими обслуживания; должностным лицам организаций, заключившим договор на предоставление услуг, в рамках договорных отношений по предоставлению услуг компании.
2. Порядок и правила предоставления доступа к объектам компании должны определяться следующими документами: регламентом (положением, инструкцией) о порядке и правилах предоставления доступа к объектам компании в рамках оказания услуг; договорными отношениями при оказании услуг и в ходе технической поддержки; должностными инструкциями сотрудников (работников) компании; приказами о режиме допуска в помещения.
3. Доступ к информационной инфраструктуре компании должен быть предоставлен специалистам и сотрудникам (работникам) только в объеме, необходимом для выполнения ими своих должностных обязанностей. Объем прав доступа специалистов и сотрудников (работников) должен быть определен исходя из назначенной им роли пользователя.
4. С целью разграничения прав доступа специалистам и сотрудникам (работникам) к объектам используются роли безопасности. Каждой роли соответствуют определенные права доступа субъекта к объекту – авторизованный пользователь.
5. Ролевое деление авторизованных пользователей реализовано с помощью функциональных возможностей разграничения доступа ПО и СКЗИ (средств криптографической защиты информации).
6. Разграничение доступа к информационной инфраструктуре осуществляется с помощью средств управления правами доступа к соответствующим ресурсам. К ним относятся: групповые политики (GPO) службы каталогов корпорации Microsoft (Active Directory); средства управления доступом ОС семейства Linux; средства управления доступом к Интернет-порталу; средства управления доступом к серверу электронной почты; средства управления доступом к серверу обмена данными; средства управления доступом к базам данных; средства управления доступом к системе хранения данных; средства управления доступом к ресурсам локальной вычислительной сети; средства управления доступом к КПТС, ПО, СКЗИ и иным сервисам, которые предоставлены специалистам, сотрудникам (работникам) в рамках выполнения должностных обязанностей и договорных отношений.
7. Разграничение доступа к вышеуказанным ресурсам включает в себя: регистрацию и идентификацию пользователей; аутентификацию пользователей; авторизацию пользователей для получения доступа к ресурсам; регистрацию и учет попыток доступа к защищаемым ресурсам.
8. При определении полномочий каждого авторизованного пользователя должны выполняться следующие условия: полномочия пользователя должны строго соответствовать его должностным обязанностям и осуществляться только в границах этих полномочий; полномочия пользователя должны распространяться на конкретные категории информации и информационных ресурсов.
9. Ответственность за допуск и назначение полномочий авторизованного пользователя к объектам Предприятия несет руководитель структурного подразделения, определивший назначение полномочий данного пользователя в докладной записке.
10. Реализацию правил разграничения доступа пользователей к объектам компании выполняет администратор информационной безопасности. Он также осуществляет контроль за соблюдением правил генерации и смены паролей доступа пользователей.
11. В компании поддерживаются следующие роли безопасности: роль «Администратор информационной безопасности», «Системный администратор» и «Пользователь». Администратор информационной безопасности уполномочен определять конфигурацию СКЗИ. Системный администратор уполномочен определять и выполнять конфигурацию ПО в соответствии со своими должностными обязанностями и полномочиями, определенными должностными инструкциями.
12. Назначение ролей пользователей информационной инфраструктуры должно выполняться исходя из выполняемых ими функциональных обязанностей. Для каждой роли в отношении единицы ресурса должен быть определен перечень допустимых операций. Допускается совмещение нескольких ролей одним сотрудником (работником) по функциям, не оказывающим влияния на уровень безопасности объекта.
13. Совмещение ролей системного администратора и администратора информационной безопасности запрещено.
14. В случае определения сотруднику (работнику) новой роли его права доступа к защищаемым данным и информационной инфраструктуре должны пересматриваться, а в необходимых случаях – блокироваться. В случае перевода сотрудника (работника) в другой отдел его права доступа к защищаемым данным и информационным системам должны пересматриваться, а в необходимых случаях – блокироваться. В случае увольнения сотрудника (работника) его права доступа к защищаемым данным и информационным системам Предприятия должны быть заблокированы.

Для организации дистанционной работы туристической компании начальники структурных подразделений разрабатывают минимальный перечень ресурсов (сервисов), доступ к которым необходим для исполнения должностных обязанностей сотрудниками структурного подразделения.

Перечень ресурсов (сервисов), согласованный с руководством направляется в управления технического развития для проектирования и создания схемы дистанционного доступа к указанным ресурсам (сервисам).

Для обеспечения дистанционной работы с ресурсами системным администратором могут создаваться дополнительные средства аутентификации сотрудников компании. Дистанционный доступ должен быть организован посредством применения средств защиты информации, имеющих сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы.

Для доступа к защищаемой информации или информационным системам обязательно должны применяться СКЗИ, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь.

Важно также предупредить и внутренние угрозы – умышленные или случайные нарушения политики информационной безопасности сотрудниками компании. Эти риски можно минимизировать, установив доступ к корпоративной информации в зависимости от уровня полномочий сотрудников. Например, менеджер по продажам располагает сведениями только о своих клиентах, а полная база и вся история продаж будет доступна только начальнику отдела продаж. Главный бухгалтер должен иметь доступ только к бухгалтерской отчетности, а управленческая отчетность будет доступна только гендиректору. Конечно, в маленькой компании добиться полного обособления функций сложно, но попытаться разграничить потоки информации между сотрудниками все-таки необходимо. Все это также снизит вероятность утечки и хищения данных.

**Вывод**

Политика безопасности – это набор управленческих решений, задачей которых является защита информации и соответствующих ресурсов. Она устанавливает технические требования для обеспечения безопасности компьютерных систем и сетей, а также определяет способы настройки систем с точки зрения безопасности.

Политика безопасности является важным аспектом для любой организации, поскольку потеря данных или их несанкционированное использование может иметь серьезные финансовые и репутационные последствия. Поэтому необходимо вкладывать достаточные ресурсы в разработку и реализацию политики безопасности, поскольку затраты на нее незначительны по сравнению с потенциальными убытками.

В политику безопасности включаются различные меры, которые обеспечивают защиту информации и ресурсов организации:

* Технические меры обеспечения безопасности включают использование безопасного программного обеспечения, установку межсетевых экранов, шифрование данных и контроль доступа. Эти технические средства обеспечивают защиту от внешних угроз и предотвращают несанкционированный доступ к информации.
* Организационные меры обеспечения безопасности включают установление правил и политик для сотрудников, проведение обучения и повышение осведомленности о безопасности информации. Также назначаются ответственные лица за безопасность и разрабатываются процедуры для обеспечения безопасности данных.
* Сетевая безопасность направлена на защиту сетей организации от несанкционированного доступа. Это включает установку протоколов безопасности, мониторинг сетевой активности и другие меры, чтобы предотвратить несанкционированный доступ к информации.
* Общие меры предосторожности, такие как регулярное резервное копирование данных, использование антивирусного программного обеспечения и обеспечение физической безопасности помещений и оборудования, также важны для защиты информации от угроз.
* Люди и процессы играют важную роль в обеспечении безопасности. Обучение сотрудников правилам безопасного поведения, разработка и реализация процедур безопасности, аудит безопасности и др. помогают предотвратить утечку данных.
* Избыточность и непрерывность работы включают наличие резервных систем и процессов, а также разработку планов действий в чрезвычайных ситуациях. Это помогает обеспечить непрерывность работы систем и минимизировать временные простои.

Разработка и реализация мер по обеспечению информационной безопасности должны быть непрерывными и не зависеть от роли IT-инфраструктуры в производственных процессах. Комплексный подход, который включает привлечение сторонних специалистов, позволит предотвратить утечку данных, а не только реагировать на ее последствия.