Учреждение образования

«Белорусский государственный технологический университет»

**Практическое задание №2**

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

Выполнил:

Студент 2 курса 2 группы ФИТ

Турчинович Никита

**Цель**: разработать проект политики информационной безопасности бизнес-компании.

**Введение**

Под понятием «политика безопасности» понимается набор документированных управленческих решений, направленных на обеспечение защиты информации и связанных с ней ресурсов. Эта политика определяет стратегию организации в области информационной безопасности, а также определяет, какое внимание и какие ресурсы руководство считает целесообразным выделять для этой цели. Все это включает в себя документированные принципы, правила, процедуры и методы, регулирующие управление, защиту и распределение важной информации. Кроме того, в политике безопасности содержатся требования к субъектам информационных отношений, а также определяется политика ролей этих субъектов.

Из-за возможности утечки информации или небрежного поведения сотрудников компания может потерять свою конкурентоспособность на рынке. Однако разработка систем защиты позволяет снизить этот риск или даже полностью избежать его. При создании таких систем необходимо руководствоваться различными стандартами, которые обеспечивают согласованное взаимодействие с государственными органами и партнерами за рубежом в соответствии с действующим законодательством.

Главная цель политики безопасности заключается в документировании правил внутри организации в области информационной безопасности. Без такой политики взаимодействие сотрудников с различными ресурсами будет регулироваться неформально, что увеличит риски нарушений и утечек данных. В результате минимизации этих рисков компания сможет увеличить свою прибыльность.

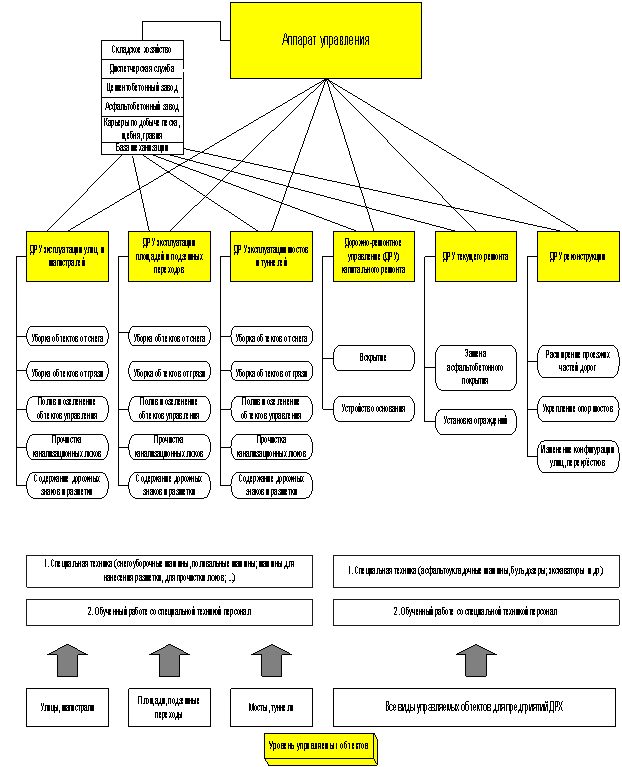
**Описание структуры компании**

Организационная структура компании представляет собой, по сути, руководящий документ, который поясняет, как организация устроена и как её деятельность организована. Для более точного определения, организационная структура определяет процесс принятия решений в компании и идентифицирует лидеров внутри неё.

Причины необходимости разработки организационной структуры предприятия:

* Организационная структура обеспечивает ясное представление о направлении движения компании. Четкая структура служит средством поддержания порядка при принятии решений и урегулировании разногласий.
* Организационная структура объединяет участников организации. Благодаря ей, новые члены группы получают определенные характеристики, и, в свою очередь, группа приобретает свои собственные особенности.
* Организационная структура независимо формируется внутри любой организации. Сама по себе организация подразумевает наличие определенной структуры.

Организационная структура Дорожно-ремонтной службы.



Основные принципы, на которых строится информационная система управления Дорожно-ремонтной службой, включают следующие аспекты:

1. Создание единой корпоративной сетевой инфраструктуры и центра управления разработками, которые способствуют автоматизации задач, перед которыми стоит Дорожно-ремонтная служба.
2. Разработка системы, обеспечивающей доступ ко всем информационным ресурсам Дорожно-ремонтной службы.
3. Управление служебными процессами с использованием информационных ресурсов.
4. Управление персоналом.
5. Применение современных технологий для разработки, управления и обслуживания всех сетевых ресурсов, используемых Дорожно-ремонтной службой, а также для правильного редактирования и заполнения этих ресурсов.
6. Поддержка информационных ресурсов, обеспечивающих комфортную работу персонала.
7. Управление документооборотом;
8. Выделение достаточных ресурсов для бесперебойной работы всей сети Дорожно-ремонтной службы.

Информационная система Дорожно-ремонтной службы позволяет собирать, анализировать и систематизировать данные о текущем состоянии дорожной инфраструктуры: количество дорожных участков, виды работ по ремонту и обслуживанию, а также другая важная информация. Некоторые функции программы единой информационной системы Дорожно-ремонтной службы позволяют отслеживать состояние дорожной техники, запланированные и завершенные проекты по ремонту дорог, и общее состояние дорожной сети.

Возможности информационной системы Дорожно-ремонтной службы позволяют четко представить структурную организацию дорожно-ремонтных бригад и всей службы в целом. Это помогает эффективно координировать работы на дорогах и взаимодействовать с другими организациями и инстанциями, а также обеспечивать своевременное информирование общества о состоянии дорожной инфраструктуры. Также это позволяет проводить обучение сотрудников в сфере дорожно-ремонтных работ.

Система Дорожно-ремонтной службы также взаимодействует с различными информационными ресурсами, электронными образовательными платформами и технологическими средствами для обеспечения оперативной передачи данных и координации работ на дорогах. Все это необходимо для выполнения задач по обслуживанию и ремонту дорожной инфраструктуры с максимальной эффективностью и прозрачностью перед обществом.

**Основные угрозы и их источники**

С каждым годом способы, с помощью которых наносится ущерб информационным системам, становятся более сложными и изменчивыми. Возрастает использование специально разработанных программ и скрытых угроз, в то время как традиционные методы атак часто устраняются при создании программ и, следовательно, перестают быть эффективными для эксплуатации. Эти угрозы все чаще проникают внутрь сетей на различные уровни, включая ядро и уровень доступа пользователей, где уровень защиты может оставаться недостаточным. Исходя из этой позиции, угрозы легко могут перейти на более высокий уровень и, в конечном итоге, достигнуть своей цели, будь то конкретные ресурсы в сети или ценная информация. Главной целью современных кибератак, как правило, является захват ценной информации с последующим её использованием, продажей, а также возможными целями могут быть шантаж и вымогательство.

Угрозы безопасности могут быть классифицированы по следующим признакам:

1. По природе возникновения (искусственные и естественные);
2. По степени преднамеренности (случайные и преднамеренные);
3. По аспекту информационной безопасности;
4. По компонентам, на которые нацелена угроза;

Для информационной системы Дорожно-ремонтной службы существуют следующие угрозы:

1. Несанкционированный доступ к конфиденциальным данным о состоянии дорожной инфраструктуры, планам ремонта, и другой важной информации. Это может привести к утечке чувствительных данных и нарушению планов по обслуживанию дорог.
2. Распространение вредоносного программного обеспечения и нежелательного контента с использованием информационных ресурсов Дорожно-ремонтной службы. Это может привести к нарушению нормального функционирования системы и угрожать целостности данных.
3. Кибертерроризм и атаки на информационную инфраструктуру Дорожно-ремонтной службы. Создание сильной защиты информационных технологий помогает предотвратить кибератаки и обеспечивает безопасное функционирование системы.
4. Хранение персональных данных сотрудников и информации о дорожной технике на компьютерах администрации. Эта информация должна быть надежно защищена от несанкционированного доступа.
5. Физические атаки на компьютеры и сервера Дорожно-ремонтной службы. Недостаточная физическая защита может позволить злоумышленникам получить доступ к данным, скопировать их на носитель и уйти незамеченными.
6. Непосредственная угроза со стороны персонала, который может скопировать данные на съемные носители или передать их через незащищенные каналы связи. Этому также необходимо уделять внимание при обеспечении безопасности информационной системы Дорожно-ремонтной службы.

Основные объекты, которые нуждаются в особой защите от несанкционированного доступа в информационной системе Дорожно-ремонтной службы, включают:

1. Локальные сети, используемые бухгалтерскими службами для учета финансовых операций и бюджетирования дорожно-ремонтных проектов.
2. Данные и ресурсы финансового отдела, где хранится конфиденциальная информация о финансовом состоянии и бюджетировании Дорожно-ремонтной службы.
3. Серверы с базами данных, содержащими информацию о состоянии дорожной инфраструктуры, планах ремонта и обслуживания, а также технических характеристиках дорожной техники.
4. FTP сервера, используемые для передачи больших объемов данных и документов между дорожно-ремонтными бригадами и центральным управлением.
5. Компьютеры, на которых хранится важная информация, такие как компьютеры командиров и руководителей бригад, где содержится информация о графиках работ, технических характеристиках оборудования и другие важные данные, необходимые для координации работ на дорогах.

Обеспечение безопасности и защиты от несанкционированного доступа к этим объектам является приоритетной задачей для обеспечения нормального функционирования и сохранности данных Дорожно-ремонтной службы.

**Оценка рисков**

Компьютерные сети Дорожно-ремонтной службы представляют собой совокупность сетевых ресурсов, необходимых для эффективной организации рабочего процесса, координации дорожно-ремонтных работ и обеспечения связи между сотрудниками.

В контексте информационной безопасности, источниками угроз для таких сетей могут стать компьютеры, используемые в рамках служебной деятельности, но при этом имеющие доступ к локальным или глобальным сетям Интернета. Это может создавать потенциальные уязвимости, через которые злоумышленники могут попытаться получить несанкционированный доступ к системам и данным Дорожно-ремонтной службы.

Особую опасность представляют случаи халатности или недостаточной информационной грамотности сотрудников, которые, имея доступ к важным документам и данным, могут неосторожно обращаться с информацией и создавать риски для ее утечки в сеть. Важно обеспечивать обучение и повышение информационной грамотности персонала, а также установить строгие политики и меры безопасности для защиты данных и сетевых ресурсов Дорожно-ремонтной службы.

Процесс анализа информационных рисков может быть разделен на следующие этапы:

1. Ранжирование объектов, требующих защиты, по их значимости.
2. Идентификация основных направлений потенциальных атак и разработка планов восстановления сети в случае её сбоя.
3. Оценка эффективности существующих методов защиты и их адаптация для обеспечения надежной работы при возможной несанкционированной атаке.
4. Выявление имеющихся или потенциальных уязвимостей и определение способов их устранения.
5. Оценка потенциального ущерба, который может быть причинен при успешной или неуспешной несанкционированной атаке на сеть.
6. Рассмотрение возможности повреждения оборудования и возникновения сбоев при различных случайных и непредвиденных ситуациях.

Базовый анализ рисков представляет собой анализ, проводимый в соответствии с минимальными требованиями безопасности. При этом методы анализа рисков на этом уровне обычно не учитывают стоимость ресурсов и не оценивают эффективность контрмер. Такие методы используются в случаях, когда не требуется повышенная безопасность информационной системы.

Полный анализ рисков, с другой стороны, применяется для информационных систем, для которых установлены высокие требования по безопасности. Он включает в себя определение стоимости информационных ресурсов, анализ угроз и уязвимостей, выбор соответствующих контрмер и оценку их эффективности.

При анализе рисков оценка ожидаемого ущерба в случае реализации угрозы сравнивается с затратами на меры и средства защиты, и на основе этой оценки принимается решение относительно управления риском, которое может включать в себя следующие варианты:

1. Снижение риска путем внедрения средств защиты, которые снижают вероятность атаки или уменьшают потенциальные убытки.
2. Исключение риска путем отказа от использования уязвимых ресурсов или технологий.
3. Передача риска, например, через страхование, где убытки будет компенсировать страховая компания.
4. Принятие риска, если он оценивается как приемлемый или несущественный.

**Разработка мер защиты и мероприятий по внедрению политики безопасности**

Борьба с различными видами атак должна вестись на пяти уровнях, при этом защита должна иметь комплексный характер в информационной системе Дорожно-ремонтной службы:

1. Внедрение антивирусного программного обеспечения.

Установка антивирусных программ позволяет обеспечить базовую защиту от вредоносных программ и вирусов, которые могут угрожать безопасности информации и работоспособности системы Дорожно-ремонтной службы.

1. Поведенческая аналитика пользователей (UBA).

Эта технология собирает информацию о действиях пользователей и анализирует их поведение на предмет несоответствий базовым нормам. Это позволяет выявлять потенциальные угрозы и действовать активно.

1. Система обнаружения вторжений (IDS) и система предотвращения вторжений (IPS), а также firewall.

IDS мониторит входящий трафик и выявляет потенциальные угрозы, в то время как IPS реагирует на подозрительный трафик и блокирует его. Файрволл служит для фильтрации трафика и предоставления данных системам мониторинга и обнаружения.

1. Морально-этические средства обеспечения информационной безопасности.

Важную роль играют правила этического поведения и моральные нормы среди сотрудников Дорожно-ремонтной службы. Они помогают предотвратить распространение незаконной или некорректной информации.

1. Административно-организационные меры.

Создание внутренних правил и регламентов, определение порядка работы с информацией и носителями, а также обучение сотрудников и мониторинг их действий важны для обеспечения безопасности данных.

1. Физические меры.

Контроль доступа в помещения, установка систем пропускной системы, использование паролей и их регулярная смена обеспечивают физическую защиту информации.

1. Технические меры.

Программное обеспечение, контролирующее доступ к сайтам с нежелательным содержанием, защита данных на жестких дисках компьютеров, а также обновление системных компонентов и антивирусного ПО помогают обеспечить техническую безопасность.

Обеспечение безопасности информации в системе Дорожно-ремонтной службы требует комплексного подхода и постоянного мониторинга, чтобы минимизировать риски и обеспечить надежную защиту данных и инфраструктуры.

**Вывод**

Информационная безопасность является одной из проблем, с которой столкнулось современное общество. Основная проблема в информационной безопасности заключается в нахождении различных уязвимостей ежедневно. Также не всегда есть возможность не жертвовать частью информации для сохранения какой-то более важной части. Кроме этого, злоумышленнику достаточно быть правым лишь один раз, а специалисту по защите нужно быть правым всегда.

Каждый раз при построении системы защиты информации нужно определять, что нужно защищать и от чего. Кроме всего этого следует защищаться не от одной конкретной угрозы, а от целого множества угроз, при этом учитывая различные факторы, которые могут присутствовать при защите информации сети или информации от злоумышленника.

Одни из обязательных этапов является проектирование системы защиты. Для корректного проектирования необходимо поставить себя на место злоумышленника для понятия того, как может действовать злоумышленник, а также какие способы несанкционированного доступа могут быть ему доступны в данном объекте или сети. Также можно попытаться самостоятельно защитить свой объект хотя бы от базовых атак, а после переходить к более узким атакам. Или провести стресс тест для оборудования, однако данные манипуляции необходимо выполнять, когда все предупреждены, иначе есть возможность из-за данного теста потеря важных документов или вовсе сбой всего оборудования по различным причинам. Кроме всего перед началом проверки следует сделать резервное копирование всей необходимой информации.

Для предупреждения успешных атак необходим постоянный поиск и анализ уязвимостей системы. Благодаря анализу уязвимостей можно обеспечить грамотную защиту необходимого ресурса. Благодаря периодическому анализу уже защищённых объектов, можно обнаружить некоторые бреши в защите или просто удостовериться в работе старых.