Учреждения образования

«Белорусский государственный технологический университет»

**Лабораторная работа №1**

**Разработка и внедрение политики безопасности оператора мобильной связи**

Выполнил:

Студент 3 курса 1 группы ФИТ

Шумова Елизавета Игоревна

# **Введение**

Услуги сотовой связи предоставляются абонентам компаниями операторами. Для этого используются базовые станции, которые соединены между собой и составляют общую зону покрытия связи оператора. Абоненты могут передвигаться между станциями без потери сигнала и прерывания связи. Кроме того, все базовые станции передают информацию системам обработки, хранения, фильтрации и резервирования данных. Оператор имеет доступ к персональным данным клиентов, распространение которых он не должен допускать. Поэтому одним из требований к системам обработки данных оператора связи является конфиденциальность данных, передаваемых пользователями сети. Для этих целей используется политика конфиденциальности компании, которая прописывается в специальном документе. Сама политика раскрывает, какие именно персональные данные, чьи и каким образом обрабатываются компанией. Цель данного документа – уведомить возможного клиента о том, что в отношении его личных данных предпринимаются все возможные технические меры по защищенному хранению, использованию и прочей обработке. Защита персональных данных не является единственным условием полноценного функционирования компании оператора мобильной связи. Существуют и другие внешние и внутренние факторы, которые предоставляют угрозу программной и информационной системе компании.

Среди них можно выделить:

– SMS-спам;

– подозрительные действия абонента;

– преднамеренное распространение корпоративных данных;

– нежелательная информация для абонентов сети;

– нарушение целостности данных;

– непредвиденная потеря данных;

– нарушение работы узлов связи.

Таким образом, оператор связи должен предоставить необходимый комплекс мер по предотвращению угроз, описанных выше, а также ряда некоторых других.

# **1 Объекты защиты Политики безопасности**

Информационная (информационно-вычислительная) система – организационно упорядоченная совокупность документов, технических средств и информационных технологий, реализующая информационные (информационно-вычислительные) процессы.

Объект – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию.

Субъект – активный компонент системы, который может инициировать поток информации.

Объектами защиты политики безопасности оператора мобильной связи являются рабочие станции, сервер и базы персональных данных абонентов.

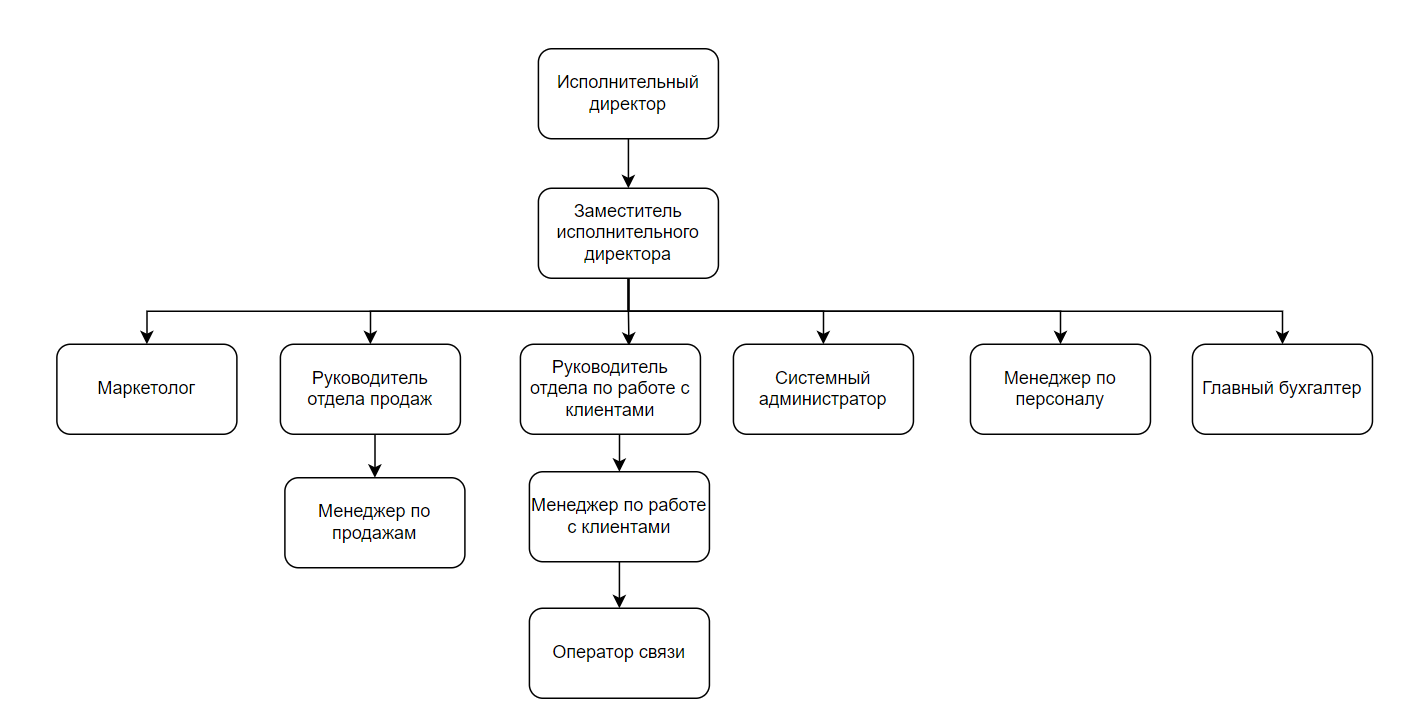


Рис.1 – Организационная структура оператора мобильной связи

# **2 Угрозы информационной безопасности оператора мобильной связи**

1. *Несанкционированный доступ к информации* – кто-либо, кроме администратора изменяет информацию, способствует ее утечке, несанкционированно изменяет параметры и настройки оборудования либо сети.
2. *Неисправность технического оборудования и программного обеспечения* – устаревшее ПО замедляет работу и препятствует качественному хранению и обработке информации.
3. *Нарушение конфиденциальности* – информация попадает в руки злоумышленников.

# **3 Оценка рисков**

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск  (Ущерб x Вероятность) |
| Спам | 1 | 0,4 | 0,4 |
| Копирование жесткого диска из центрального офиса | 3 | 0,1 | 0,3 |
| Повреждение кабелей связи | 3 | 0,2 | 0,6 |
| Утечка персональных данных | 4 | 0,1 | 0,4 |
| Нарушение работы базы данных | 3 | 0,1 | 0,3 |
| Вирусная атака | 1 | 0,2 | 0,2 |
| Итого |  |  | 2,2 |

# **4 Разработка мер защиты**

В целях предотвращения несанкционированного доступа к информации и ее утечки, хищения технических средств обработки и хранения информации и несанкционированного управления ими обеспечивается физическая защита входящих в нее технических средств. Серверное оборудование и критичное сетевое оборудование размещаются в запираемых шкафах с сигнализацией, располагаемых в специализированных помещениях (серверных), ограничивающих доступ к ним посторонних лиц. Перед утилизацией или передачей в ремонт технических средств выполняется гарантированное удаление информации с них. Кабельные сети прокладываются так, чтобы максимально ограничить несанкционированный доступ к ним. Для защиты от перебоев электричества в эксплуатацию вводятся централизованные системы бесперебойного питания.

Доступ в помещения ограничивается средствами контроля и управления доступом.

Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации разделяются и возлагаются на специально выделенных для этого работников. Изменения конфигурации средств обработки и хранения информации, а также изменения сетевой инфраструктуры, конфигурации сетевого оборудования выполняются администратором. Все изменения регистрируются в соответствующих журналах. Самостоятельное изменение конфигурации средств обработки, хранения и передачи информации пользователями запрещено. Использование съемных носителей информации в автоматизированной системе управления технологическими процессами запрещено. При размещении средств разработки, тестирования и эксплуатации обеспечивается их физическое или логическое разделение в целях снижения риска несанкционированного доступа или внесения изменений в систему.

В целях предотвращения проникновения, обнаружения внедрения и нейтрализации вредоносного ПО применяются средства защиты от вредоносного ПО. Администрирование средств защиты от вредоносного ПО осуществляется системным администратором.

В целях обеспечения непрерывного и устойчивого функционирования осуществляется защита ее сетевой инфраструктуры. Защита сетевой инфраструктуры обеспечивается:

– физической защитой сетевого оборудования и средств защиты;

– контролем логического доступа к сетевому оборудованию;

– шифрованием каналов управления;

– контролем сетевых соединений;

– обнаружением и предотвращением вторжений;

– использованием встроенных в сетевое оборудование средств защиты от подмены адреса (средств антиспуфинга);

– защитой информации ограниченного доступа при ее передаче вне контролируемых зон;

– применением средств мониторинга и регистрации событий.

Категорически запрещается удаленное администрирование.

В целях поддержания работоспособности ПО осуществляются меры по устранению уязвимостей ПО, а также другие меры защиты от:

– умышленного либо неумышленного раскрытия, модификации или уничтожения защищаемых данных. В частности, это подразумевает использования средств ограничения доступа к различным ресурсам офисного контроля;

– установки средств защиты кем-либо, кроме администратора, несанкционированного внесения изменений в порядок функционирования системы защиты, изменения ее возможностей. Данное требование приводит к необходимости разграничения прав доступа к настройкам системы, защите ее от несанкци­онированного воздействия. Это подразумевает использование в локальной сети только программных продуктов, поддерживающих ролевой принцип доступа, а также применение функций офисного контроля. Средства защиты должны устанавливаться как на рабочие станции, так и на сервер. В организации, соответствующей требованиям стандарта, должна использо­ваться только защищенная почта, что вместе с требованием о наличии защиты от вирусов и спама подразумевает установку средств антивирусной фильтрации почтовых сообщений. Обновление ОС, другого общесистемного и прикладного ПО осуществляется системными администраторами и администраторами прикладных систем. Обновления для ПО получаются с серверов обновлений.

В целях обеспечения конфиденциальности информации при ее передаче вне контролируемых зон применяются сертифицированные установленным порядком средства криптографической защиты информации. Это специальные методы шифрования, кодирования в результате которых содержание передаваемых файлов становится недоступным, без предъявления ключа криптограммы и обратного преобразования. Криптографическая защита информации на предприятии реализована с помощью метода криптосистемы с открытым ключом. В системе с открытым ключом используются два ключа — открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

В целях обеспечения безопасности информационных ресурсов и устойчивого функционирования осуществляется управление доступом пользователей к операционным и прикладным системам, а также сетевому оборудованию. Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач. Наделение пользователей правами доступа и привилегиями основывается на установленной в компании формализованной процедуре предоставления прав доступа. Права доступа и привилегии пользователей подлежат регулярному пересмотру. Каждый пользователь обеспечивается уникальным персональным идентификатором. Подтверждение подлинности идентификатора (аутентификация) пользователя осуществляется при помощи паролей и/или средств усиленной аутентификации. Длина, сложность и срок действия паролей устанавливаются в зависимости от степени критичности защищаемых систем.

# **Выводы**

Политика безопасности — совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Основная цель политики безопасности – определение технических требований к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности.

На политике безопасности нельзя экономить, так как данные, которые могут быть подвержены хищению, копированию или изменению, могут стоить дороже, чем ресурсы, потраченные на её разработку и осуществление.

Разработаны технические меры обеспечения безопасности, организационные меры обеспечения безопасности, сетевая безопасность, общие меры предосторожностей.

Политика безопасности должна быть разработана так, чтобы её взлом стоил дороже, чем сама информация.­