Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа № 1**

По теме «Разработка политики информационной безопасности оператора мобильной связи»

Студент: Шулаков А. А.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

# 1. Обоснование актуальности, цели и задачи разработки ПИБ в организации (учреждении)

***Политика информационной безопасности (ПИБ) организации или учреждения*** – совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

**Актуальность ПИБ** состоит в том, чтобы не допустить законодательно или на основе правил утечки конфиденциальной информации оператора мобильной связи в свободный доступ.

**Цели:**

* Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
* Создание единой системы взглядов и понимания целей, задач и принципов обеспечения информационной безопасности;
* Реализацию права на доступ к информации.

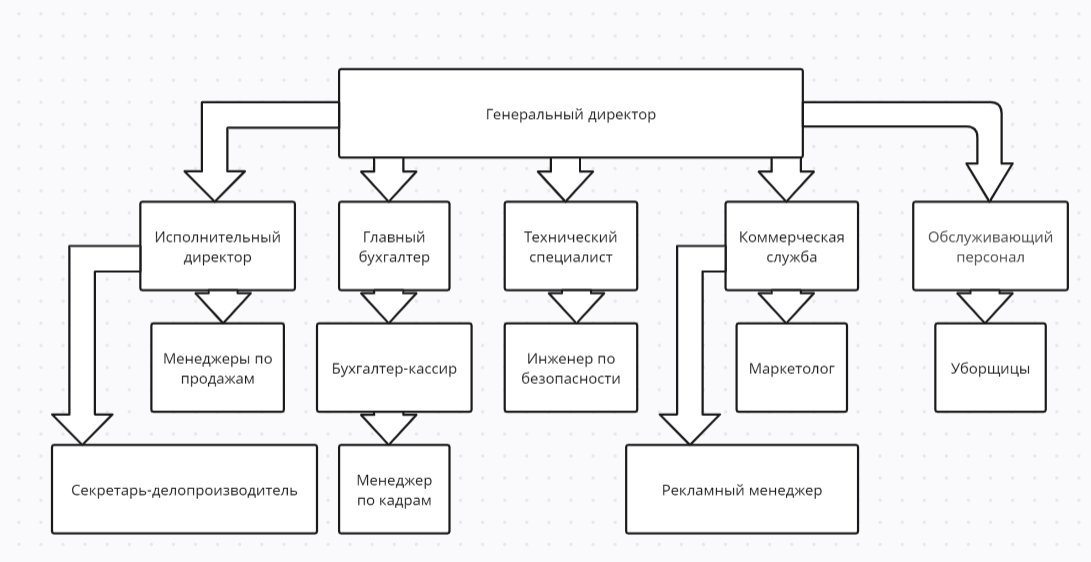
**Задачи:**

* Разработка концепции, стандартов, процедур, инструкций и планов мероприятий по обеспечению надёжности и безопасности информационных средств в компании оператора мобильной связи;
* Описание структуры компании оператора мобильной связи и характеристика всех возможных объектов и субъектов защиты;
* Обеспечение информационной безопасности на предприятии;
* Оценивание рисков на основании вероятности возникновения и возможного ущерба от потенциальных угроз;
* Разработка мер, методов и средств обеспечения необходимого уровня защищённости информации в страховой компании.

# 2. Объекты защиты

По варианту необходимо разработать политику безопасности для опера-тора мобильной связи.

Рисунок 1 – структура компании оператора мобильной связи



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

**Объекты защиты**:

* Коммерческая тайна самого оператора мобильной связи, данные о его договорах, финансовых взаимоотношениях, бухгалтерская информация;
* Коммерческая тайна клиентов и партнеров организации, данные об их активах, имуществе, платежах, произошедших транзакциях (звонках, сообщениях, интернет трафике);
* Персональные данные сотрудников компании и клиентов, эта информация иногда включает номера телефонов, персональные данные, данные банковских карт.

***Субъект*** – активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

**Субъекты защиты**: владельцы, пользователи информации и поддерживающей инфраструктуры.

# 3. Основные угрозы и их источники

Все многообразие потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: *естественные* (объективные) и *искусственные* (субъективные).

***Естественные угрозы*** – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека.

***Искусственные угрозы*** – это угрозы, вызванные деятельностью человека.

***Непреднамеренные*** (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей ИВС (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов ИВС.

***Преднамеренные*** (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т. п.) действия легально допущенных к информационным ресурсам пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы.

Естественные угрозы:

* Пожары;
* Ураганы;
* Наводнения.

Искусственные угрозы:

* Непреднамеренные угрозы:
  + Ошибки пользователей и обслуживающего персонала;
  + Разговоры на тему работы.
* Преднамеренные угрозы:
  + Кражи;
  + Нападения;
  + Взлом;
  + Саботаж;
  + Проникновение в помещение;
  + Фарминг (перенаправление на фейковый ip);
  + Mailbombing;
  + Копирование архивных данных;
  + Фишинг.

Источники угроз по отношению к самой информационной системе могут быть как *внешними*, так и *внутренними*.

Внешние угрозы:

* Атаки со стороны конкурентов(удаленный несанкционированный доступ третьих лиц к информационным ресурсам страховой компании с целью получения материальной выгоды)
* Атака со стороны мошенников(физическое неправомерное нарушение целостности средств хранения важных информационных источников техногенного и естественного характера третьими лицами путём взлома, краж).

Внутренние угрозы:

* Атаки со стороны сотрудников(халатность и невыполнение поставленных обязательств; доступ к ресурсам компании ранее уволенными сотрудниками, который может повлечь утечку данных компаниям-конкурентам).

# 4. Оценка угроз, рисков и уязвимостей

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления ИБ.

Таблица 1 ­– Условная численная шкала для оценки ущерба компании

|  |  |
| --- | --- |
| **Величина ущерба** | **Описание** |
| 0 | Раскрытие информации, не являющейся конфиденциальной и не раскрывающая данных о заказчиках |
| 1 | Ущерб атаки есть, но он незначителен и не связан с положением компании на рынке |
| 2 | Существует вероятность потери некоторого числа клиентов, компания теряет часть прибыли |
| 3 | Потеря весомой доли клиентов и потеря доли рынка, компания несет убытки |
| 4 | Полная потеря рынка и конкурентоспособности, долги, а так же полная потеря клиентов, банкротство |
| 5 | Полное банкротство компании и прекращение существования |

Вероятность того, что угроза реализуется, определяется на основе следующих факторов:

* Привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* Возможность использования ресурса для получения дохода как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* Технические возможности угрозы, используемые при умышленном воздействии со стороны человека;
* Вероятность того, что угроза реализуется;
* Степень легкости, с которой уязвимость может быть использована.

Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем. Очевидно, что разработка политики безопасности требует учета специфики конкретных организаций.

Таблица 2 – Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| **Вероятность события** | **Средняя частота события (НСД)** |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

Далее проверяется каждая строка таблицы: превышен или не превышен порог для значения риска, связанного с анализируемой атакой? Если такое превышение имеет место, данная атака должна рассматриваться с точки зрения одной из первоочередных целей разработки политики безопасности.

Таблица 3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| **Атака** | **Ущерб** | **Вероятность** | **Риск** |
| Кражи | 4 | 0,1 | 0,4 |
| Нападение | 4 | 0,1 | 0,4 |
| Взлом | 4 | 0,1 | 0,4 |
| Проникновение в помещение | 4 | 0,1 | 0,4 |
| Саботаж | 4 | 0,1 | 0,4 |
| Фарминг (перенаправление на фейковый ip) | 1 | 0,2 | 0,2 |
| Mailbombing | 2 | 0,3 | 0,6 |

|  |  |  |  |
| --- | --- | --- | --- |
| Копирование архивных данных | 3 | 0,1 | 0,3 |
| Фишинг | 4 | 0,3 | 1,2 |
| Разговоры на тему работы | 2 | 0,2 | 0,4 |
| Ошибки пользователей и обслуживающего персонала | 2 | 0,2 | 0,4 |
| Итого |  |  | 5,1 |

# 5. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов

После того как документация по информационной безопасности готова, необходима плановая деятельность по ее внедрению в повседневную работу. Основу таких мероприятий, как было указано в плане выполнения лабораторной работы, составляют инструкции, содержащие подробное описание (алгоритмы) действий по организации информационной защиты и обеспечению разработанных стандартов и процедур, и план мероприятий по обучению персонала и тестированию знаний сотрудников, имеющих доступ к информационным ресурсам.

Методы обеспечения требуемого уровня защищенности информационных ресурсов:

* Проверка надежности функционирования системы защиты;
* Наблюдение за функционированием системы защиты и ее элементов;
* Контроль за соблюдением пользователями и обслуживающим персоналом установленных правил обращения с информацией;
* Контроль за действиями администраторов баз данных, серверов и сетевых устройств;
* Подготовка решений по обеспечению конфиденциальности, доступности, целостности данных;
* Принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты.

Система мер, рекомендуемая для большинства компаний, перед которыми стоит вопрос защиты информации, призвана обеспечить соблюдение основных признаков ее безопасности:

* Доступность сведений. Под этим определением понимается возможность и для авторизованного субъекта в любое время получить требуемые данные, и для клиентов в регулярном режиме получать информационные услуги;
* Целостность информации. Это означает ее неизменность, отсутствие любых посторонних, неавторизованных вмешательств, направленных на изменение или уничтожение данных, нарушение системы их расположения;
* Конфиденциальность или абсолютная недоступность данных для неавторизованных субъектов;
* Отсутствие отказа или невозможность отрицать принадлежность действий или данных;
* Аутентичность или возможность достоверного подтверждения авторства информационных сообщений или действий в системе.

# Выводы

Политика информационной безопасности неразрывно связана с развитием компании, ее стратегическим планированием, она определяет общие принципы и порядок обеспечения информационной безопасности на предприятии. Политика информационной безопасности тесно интегрируется в работу предприятия на всем этапе его существования. Все решения, предпринимаемые на предприятии, должны учитывать её требования.

Эффективное обеспечение требуемого уровня информационной безопасности организации возможно только при наличии формализованного и системного подхода к выполнению мер по защите информации. Целью разработки политики информационной безопасности организации является создание единой системы взглядов и понимания целей, задач и принципов обеспечения информационной безопасности.

Определение эффективности реализации требований безопасности является одной из ключевых задач обеспечения безопасности активов на всех этапах жизненного цикла объектов информационных технологий (ОИТ). Ее решение связано с разработкой соответствующих методик, методов и средств оценки эффективности защиты активов, которая затруднена рядом объективных факторов, обусловленных сложностью и динамичностью процессов и информационных потоков, существующих в ОИТ, стремительным развитием информационных технологий, хаотичностью возникновения новых видов угроз, приводящих к появлению новых уязвимостей аппаратных и программных средств как в самом объекте информационных технологий, так и в средствах обеспечения безопасности.

Адекватный уровень ИБ в современной организации может быть обеспечен только на основе комплексного подхода, реализация которого начинается с разработки и внедрения эффективных ПБ. Эффективные ПБ определяют необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски ИБ до приемлемой величины. Они оказывают минимальное влияние на производительность труда, учитывают особенности бизнес-процессов организации, поддерживаются руководством, позитивно воспринимаются и исполняются сотрудниками организации. Для того чтобы ПБ оставалась эффективной, необходимо осуществлять непрерывный контроль ее исполнения, повышать осведомленность сотрудников организации в вопросах ИБ и обучать их выполнению правил, предписываемых ПБ. Регулярный пересмотр и корректировка правил ПБ необходимы для поддержания ее в актуальном состоянии.

Разработка и внедрение ПБ в организации – процесс коллективного творчества, в котором должны участвовать представители всех подразделений, затрагиваемых производимыми изменениями. Координатором этого процесса является специалист, на которого руководство организации возлагает ответственность за обеспечение ИБ.