Практическая работа №3

Тема: «Использование методов безопасности для информационной системы»

Задание: составить правила безопасности для следующих категорий компаний:

* IT-компания, занимающаяся разработкой системного ПО;
* государственной компании, связанной с военно-промышленным комплексом;
* частная компания, занимающаяся Аналитикой рынка товаров (Консалтинговая компания).

**Политика безопасности организации** — совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации.

Согласно отечественному стандарту **ГОСТ Р ИСО/МЭК 17799-2005**, политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью. В соответствии с указанным стандартом, необходимо, чтобы политика [информационной](https://arinteg.ru/articles/pravovye-problemy-informatsionnoy-bezopasnosti-27627.html) безопасности предприятия как минимум включала:

-определение информационной безопасности, её общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации

-изложение целей и принципов информационной безопасности, сформулированных руководством

-краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например, таких как:

\* соответствие законодательным требованиям и договорным обязательствам;

\* требования в отношении обучения вопросам безопасности;

\* предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;

\* управление непрерывностью бизнеса;

\* ответственность за нарушения политики безопасности.

IT-компания, занимающаяся разработкой системного ПО

### Принципы обеспечения информационной безопасности

В Софтлайн определены следующие принципы обеспечения информационной безопасности:

**Принцип системности**

Активы рассматриваются как взаимозависимые компоненты единой системы. Взаимовлияние компонентов учитывается при анализе рисков и угроз информационной безопасности.

**Принцип полноты (комплексности)**

В целях обеспечения информационной безопасности используется широкий спектр мер, методов и средств защиты, комплексное использование которых обеспечивает нейтрализацию актуальных угроз и отсутствие и уязвимостей в точках интеграции.

**Принцип эшелонированности**

Недопустимо полагаться на один защитный рубеж. Система обеспечения информационной безопасности строится так, чтобы наиболее защищаемая зона безопасности находилась внутри других защищаемых зон.

**Принцип равнопрочности**

Эффективность защитных механизмов не должна быть сведена на нет слабым звеном, возникшим в результате недооценки угроз либо применения неадекватных мер защиты.

**Принцип непрерывности**

Обеспечение информационной безопасности является непрерывным целенаправленным процессом, предполагающим принятие мер защиты на всех этапах жизненного цикла активов.

**Принцип разумной достаточности**

«Абсолютная» защита активов невозможна. Выбор средств защиты, адекватных актуальным угрозам, осуществляется на основе анализа рисков.

**Принцип законности**

При выборе и реализации мер обеспечения информационной безопасности Софтлайн строго соблюдает применимое законодательство, требования нормативных правовых и технических документов в области информационной безопасности.

**Принцип управляемости**

Процессы обеспечения и совершенствования информационной безопасности должны быть управляемыми, т.е. необходимо осуществлять мониторинг, измерение параметров и своевременно корректировать процессы.

**Принцип персональной ответственности**

Ответственность за обеспечение информационной безопасности возлагается на каждого сотрудника в пределах его полномочий.

Задачи в области информационной безопасности

Для достижения целей в Софтлайн приняты следующие задачи в области информационной безопасности:

• Проектирование, внедрение и непрерывное совершенствование системы управления информационной безопасностью (далее — СУИБ).

• Вовлечение высшего руководства Софтлайн в процесс функционирования СУИБ. Вопросы информационной безопасности регулярно рассматриваются уполномоченными комитетами и/или рабочими группами.

•Эффективное использование ресурсов, выделенных в целях обеспечения информационной безопасности. Оценка эффективности расходов.

• Обеспечение безопасности информационных активов Софтлайн.

• Соблюдение законодательства, требований регулирующих организаций в области информационной безопасности и защиты персональных данных.

• Совершенствование технических, организационных и правовых мер защиты.

• Формирование, накопление и развитие компетенций в области информационной безопасности и защиты персональных данных.

• Использование риск-ориентированного подхода. В Софтлайн регулярно проводится оценка рисков информационной безопасности и мероприятия по повышению уровня защищенности информационных активов.

• Управление инцидентами информационной безопасности. Софтлайн непрерывно совершенствует механизмы реагирования на инциденты.

• Повышение осведомленности сотрудников. Сотрудники Софтлайн регулярно проходят обязательное обучение по информационной безопасности.

• Формализация требований информационной безопасности. Требования фиксируются в локальных нормативных актах и доводятся до сотрудников.

• Учет требований информационной безопасности в проектной деятельности. Разработка и документирование требований к обеспечению информационной безопасности осуществляется на начальных этапах реализации проектов.

• Проверка благонадежности сотрудников. Все кандидаты на вакантные должности проходят проверку в соответствии с установленными процедурами.

• Мониторинг и непрерывное совершенствование СУИБ по результатам периодических аудитов (проверок)