Тип работы: Курсовая работа

Предмет: Шифрование

Содержание

1.5. Класс защищенности информационной системы

В информационных системах, отнесенных к классам К1, К2, К3, необходимо применение как специальных средств защиты информации, так и организационных мер, направленных на определение ответственности сотрудников за нарушение законодательства в области защиты информации конфиденциального характера.
Таким образом, аудит информационной системы в части информационной безопасности заключается в отнесении типа обрабатываемых данных к определенному классу в соответствии с которым выбирается тип защищенности информационной системы, который определяет порядок организационно-технологических мер, применяемых на предприятии. Аудит может осуществляться:
- сторонними лицензированными организациями;
- специалистами государственных структур;
- специалистами подразделения безопасности предприятия.
Согласно проведенному исследованию, по результатам аудита информационной системы ООО «Витязь» класс информационной системы отнесен к типу К3, соответственно требования к информационной безопасности должны быть сопоставлены данному классу.

Глава 2. Правовые основы системы безопасности
2.1. Законодательные меры
Проведем обзор законодательства, регламентирующего вопросы обеспечения защиты ПДн. Перечень правовых актов, в которых определены требования в области защиты ПДн, включает [4]:
 152- ФЗ «О Персональных данных» от 27.07.2006;
 Статьи Трудового кодекса;
 Указы, постановления и ГОСТы, применяемые для решения задач защиты ПДн в системах определенного вида.
В соответствии с 152-ФЗ «О персональных данных», компании, осуществляющие обработку ПДн, должны

принимать меры, исключающие возможности несанкционированного доступа к ПДн. Определение комплекса мер по защите осуществляется в соответствии с классом защищенности, объемами обрабатываемых сведений.
В Постановлении Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»/ Приказ ФСТЭК России № 21 от 18.02.2013 определяет принципы классификации систем персональных данных. Согласно приказу ФСБ от 10.07.2014 № 378 определены четыре уровня защищенности персональных данных. Проведена детальная классификация ИСПДн, в которой определены классы защищенности ПДн по типам [6]:
- общедоступные ПДн;
- ПДн, позволяющие однозначно идентифицировать субъекта;
- ПДн, при утечке которых не наступает негативных последствий для субъекта;
- ПДн, утечка которых может приводить к негативным последствиям для их субъекта.

Для каждого из уровней защищенности определен перечень мероприятий по защите от утечек. Класс защищенности присваивается системе по результатам аудита, который проводится или сторонними сертифицированными организациями или силами специалистов компании, имеющих соответствующие компетенции.
Коммерческая тайна представляет собой любую информацию, соответствующую следующим условиям:
- включает информацию, связанную с предпринимательской деятельностью компании, что предполагает данные об используемых технологиях производства, бизнес-процессах, маркетинговых разработках, данные о клиентах и контрагентах и др.;
- не относится к категории государственной тайны;
- компания является правообладателем данной информации;
- к информации не имеют доступа сторонние лица, но при этом она может представлять для реальную ценность;
- обладателем данной информации ограничены возможности доступа к ней и принимаются меры для её защиты от несанкционированного доступа.

2.2. Административные меры

Признаки отнесения информации к категории коммерческой тайны определяются ее обладателем. Процесс выделения типов информации, отнесенных к коммерческой тайне, регламентируются законодательными актами, к которым относится Гражданский кодекс и закон о коммерческой тайне.
Коммерческая тайна — это информация, которая имеет коммерческую ценность именно потому, что неизвестна никому другому. При этом у других лиц нет к ней доступа на законном основании. При этом обязательным условием является соблюдение требований к защите от ее разглашения со стороны владельца. (п. 1 и 2 ст. 3 ФЗ «О коммерческой тайне»). Также признаком коммерческой тайны является вероятность ущерба для бизнеса обладателя в случае утечек информации, отнесенной к коммерческой тайне.
Таким образом, для соблюдения режима коммерческой тайны предполагается использование специального режима конфиденциальности информации, который дает ее обладателю ряд преимуществ. Например, позволяет увеличить доходы и избежать неоправданных расходов. Так, сведения о том, как банк проверяет получателей кредитов и по каким параметрам их оценивает, помогают отсеивать потенциальных мошенников и снижают вероятность неоправданных расходов. Или компания благодаря этому режиму сохраняет положение на рынке товаров, работ, услуг, потому что держит в секрете сведения, как формируются скидки и когда следующая акция.
Мероприятия по защите коммерческой тайны устанавливаются внутриорганизационными документами, на документах, содержащих коммерческую тайну, проставляется соответствующий гриф. При этом правила обращения с документами с подобным грифом прописываются во внутренних нормативах предприятия.
Далее определены требования к регламентации работы по определению информации, содержащей элементы коммерческой тайны. Перечень сведений данного типа в условиях предприятий может подвергаться изменениям. При этом в соблюдение режима конфиденциальности требуются финансовые вложения и стоимость защищаемых данных не должна превышать стоимость мероприятий по ее защите.
В рамках регламентации режима коммерческой тайны проводится определение списка защищаемых данных, обоснование применения к ним режима конфиденциальности, описывается порядок снятия

данного режима.
Таким образом, регламент должен содержать:
1. Описание типов информации, отнесенной к категории коммерческой тайны.
2. Указание списка лиц, имеющих доступ к работе с конфиденциальной информацией.
3. Порядок снятия грифа конфиденциальности.
Далее рассмотрим основные требования к разработке Положения о коммерческой тайне. Данный документ является обязательным, без которого отсутствуют основания для привлечения виновных к ответственности в случае нарушения требований к конфиденциальности.
В Положении указываются отсылки к нормативным актам, на основании которых вводится режим, даются толкования терминологии.
В Положении необходимо четкое определение документов и носителей информации, в которых содержится коммерческая тайна, описываются действия, приводящие к нарушению режима конфиденциальности и влекущие санкции.
Также прописываются размеры ущерба и порядок его взыскания.
В Положение включаются следующие пункты:
1. Список лиц, допущенных к работе с коммерческой тайны, обоснование ввода режима конфиденциальности, значимости этой информации в бизнесе.
2. Перечень лиц, определяющих порядок отнесение информации к категории конфиденциальной.
3. Порядок действий, которые возможны с конфиденциальной информацией.

Список использованных источников

1. Аврунев О. Е., Стасышин В. М. Бизнес-информатика. [Текст] учебное пособие: / О. Е. Аврунев, В. М. Стасышин. - Новосибирск: Изд-во НГТУ, 2018. – 121с.
2. Нестеров С. А. Базы данных: учебник / С. А. Нестеров. — Москва: Издательство Юрайт, 2022. — 230 с.
3. Гордеев С. И. Организация баз данных в 2 ч.: учебник / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 310 с.
4. Бабиева Н. А., Раскин Л. И. Автоматизация ИТ-сервисов на предприятиях. [Текст]: учебно-методическое пособие / Н. А. Бабиева, Л. И. Раскин. – М.: Инфра-М, 2018. – 208 с.
5. Баранчиков А. И. Управление ИТ-инфраструктурой организаций [Текст] : учебник / А. И. Баранчиков. - Рязань: РГУ, 2019. - 219 с.
6. Васильков, А.В. Информационные системы и их безопасность [Текст] : Учебное пособие / А.В. Васильков, А.А. Васильков, И.А. Васильков. - М.: Форум, 2018. - 528 с.
7. Гантц И. С. Разработка конфигураций в среде "1С: Предприятие»: учебно-методическое пособие / И. С. Гантц. - Москва : МИРЭА - Российский технологический университет, 2020. - 63 с.
8. Стружкин Н. П. Базы данных: проектирование : учебник для вузов / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2022. — 477 с.
9. Даева С. Г. Основы разработки корпоративных информационных систем на платформе 1С: Предприятие 8.3: учебно-методическое пособие / Даева С. Г. - Москва : РТУ МИРЭА, 2020. – 562с.
10. Зимин, В.В. Управление жизненным циклом ИТ-сервисов в системах информатики и автоматизации (лучшие практики ITIL) [Текст] : учебное пособие / В. В. Зимин. - Кемерово: Кузбассвузиздат, 2018. – 499 с.