|  |
| --- |
| Описание: Описание: для прик эмбл |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего профессионального образования  **"Российский технологический университет"**  **МИРЭА** |
| Институт «Комплексной безопасности и специального приборостроения» |
| Кафедра «Управление и моделирование систем» (КБ-3) |
|  |

|  |  |
| --- | --- |
| **Практика №1 по дисциплине** | |
|  | |
| **« Основы информационной безопасности »**  **«Политика безопасности»** | |
|  | |
| Выполнил студент группы БИСО-03-19 | *Чанышев А.Т.* |

Москва 2020

Компания ООО «ABC»

Штат — 50 сотрудников. 5 руководство, 10 бухгалтерия, 5 — IT-отдел, 25 — менеджеры по работе с клиентами, Отдел кадров – 5 сотрудников.

Руководство использует телефонную связь, MS Office, 1С: Предприятие и т. д.

Бухгалтерия использует MS Office, 1С: Бухгалтерия. Занимается формированием полной и достоверной информации о деятельности организации и ее имущественном положении.

IT-отдел занимается установкой, обеспечением правильной эксплуатации и бесперебойной работы, а также техническим обслуживанием компьютеров. Администрирование сетевых ресурсов, баз данных. Обеспечивает функционирование сайта и личных кабинетов клиентов. Имеет доступ к базам данных и к CMS.

Менеджеры по работе с клиентами осуществляют работу с ними посредством Интернет. Телефонной связи и др.

Отдел кадров использует MS Office, 1С: Зарплата и Кадры. Обеспечивает предприятие необходимыми кадрами и эффективным использованием потенциала работников.

**Политика информационной безопасности компании ООО «ABC»**

**Содержание**

[1. Общее положение 4](#_Toc54390627)

[1.1 Цель документа 4](#_Toc54390628)

[2. Цели обеспечения и управления информационной безопасностью 4](#_Toc54390629)

[3. Подход к обеспечению информационной безопасности 5](#_Toc54390630)

[4. Порядок пересмотра Политики 6](#_Toc54390631)

[5. Технический регламент для отдела безопасности 6](#_Toc54390632)

**1. Общее положение**

Обеспечение информационной безопасности является необходимым условием для осуществления деятельности интернет-магазина «ABC». Нарушение информационной безопасности может привести к серьезным последствиям для Компании, включая потерю доверия со стороны партнеров, клиентов, поставщиков и снижение конкурентоспособности.

**1.1 Цель документа**

Целью политики информационной безопасности интернет - магазина «ABC» для размещения в сети интернет является декларация основных целей и положений по организации процессов обеспечения и управления информационной безопасностью Компании.

**2. Цели обеспечения и управления информационной безопасностью**

Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

Основными целями в области обеспечения и управления информационной безопасностью Компании являются:

- Обеспечение целостности, доступности и конфиденциальности критичной информации, а также обеспечение доступности критичных ИТ-сервисов Компании.

- Применение обоснованных, экономически эффективных организационных и технических мер по обеспечению информационной безопасности.

- Соответствие Компании требованиям действующего законодательства и регуляторов в области ИБ.

- Соответствие процессов обеспечения информационной безопасности бизнес-требованиям Компании.

- Обеспечение доверия клиентов и партнеров Компании.

- Установление ответственности сотрудников по вопросам обеспечения информационной безопасности и повышение их осведомленности.

**3. Подход к обеспечению информационной безопасности**

- Информация является важным активом Компании, и ее защита является обязанностью каждого сотрудника.

- Доступ к информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.

- Сотрудники Компании проходят регулярное обучение в области информационной безопасности.

- В Компании регулярно проводится независимый аудит информационной безопасности.

- Специалисты информационной безопасности отвечают за определение детальных требований информационной безопасности и контролируют их исполнение в Компании.

- Меры защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.

- Меры защиты персональных данных внедряются согласно требованиям Федерального закона № 000 «О защите персональных данных» и других нормативных документов, регламентирующих обработку персональных данных в автоматизированных и неавтоматизированных информационных системах.

- Оценка рисков информационной безопасности проводится ежегодно, а также в случае значительных изменений в структуре Компании и ее бизнес-процессах.

- При оценке рисков учитывается влияние реализации угроз информационной безопасности на финансовое положение Компании и ее репутацию на рынке.

- Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

- Успешное достижение целей настоящей политики возможно только при выполнении положений регламентов информационной безопасности.

**4. Порядок пересмотра Политики**

Политика должна пересматриваться при наступлении существенных событий, но не реже чем один раз в три года.

**5. Технический регламент для отдела безопасности**

1) Исключение возможности доступа третьих лиц к документам, содержащим конфиденциальную информацию.

2) Контроль за соблюдением установленного уровня доступа внутри компании.

3) Соблюдение требований и правил по работе со средствами технической защиты, в том числе со средствами криптографической защиты.

4) Контроль состояния автоматизированной системы и реагирование на ситуации, имеющие характер инцидентов ИБ, а именно: нарушения целостности пломб, свидетельствующие о попытке проникнуть в охраняемую зону, некорректном срабатывании антивирусной защиты, нарушения в работе программного обеспечения, выявленных изменениях файлов, выходе из строя периферийных устройств.

5) Исключение копирования любых файлов или текстовой информации в любых целях без получения санкции руководителя.

6) Обеспечение антивирусной безопасности.

7) Обеспечение безопасности персональных данных. А именно:

- Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.

- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

- Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.