|  |  |  |
| --- | --- | --- |
| |  | | --- | | МИНОБРНАУКИ РОССИИ | | Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |   **Институт комплексной безопасности и специального приборостроения (ИКБСП)** |
|  |

|  |  |
| --- | --- |
| **ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ № 1** | |
| по дисциплине  «Основы информационной безопасности» | |
| ВВыполнил студент группы БИСО-01-19 | Попова Наталья Викторовна |
|  |

Аккаунт github: <https://github.com/Kometulus>

Москва 2020

Компания ООО «Облако». Штат - 66 сотрудников. 7 - руководство, 10 - бухгалтерия, 5 - IT-отдел, 30 - менеджеры по работе с клиентами, 6 - отдел безопасности,3 - отдел маркетинга, 5 - отдел физической безопасности.

Управляющая часть компании использует телефонную связь, MS Office, 1С: Предприятие и т. д.

Бухгалтерия использует телефонную связь, MS Office, 1С: Бухгалтерию.

IT-отдел обеспечивает функционирование внутренней сети организации, а также сайта компании и личных кабинетов клиентов.

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

Отдел безопасности обеспечивает целостность и сохранность личных данных клиентов и компании.

Отдел маркетинга обеспечивает конкурентоспособность, разработку новых товаров и услуг, различные исследования и аналитику и др.

Отдел физической безопасности обеспечивает охрану от доступа посторонних лиц, защиту имущества компании и защиту сотрудников.

1. **Общие положения**

Настоящая Политика разработана в соответствии с требованиями законодательства Российской Федерации и нормами права в части обеспечения информационной безопасности. Основывается, в том числе на:

* Федеральном законе №149-ФЗ от 27.06.2006 «Об информации, информационных технологиях и о защите информации»;
* Федеральном законе №152-ФЗ от 27.06.2006 «О персональных данных»;
* Доктрине информационной безопасности Российской Федерации №646 от 05.12.2016;
* Внутренних нормативно-методических и организационно-распорядительных документах.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Целью документа является защита интересов ООО «Облако», его клиентов и партнеров, а также обеспечение стабильной работы путем определения процесса обеспечения информационной безопасности, соответствующего потребностям бизнеса и минимизации воздействия на бизнес Организации со стороны инцидентов информационной безопасности.

Настоящая Политика распространяется на все структурные подразделения ООО «Облако» и обязательна для применения всеми сотрудниками и руководством, а также пользователями его информационных ресурсов. Требования настоящей Политики могут развиваться другими внутренними нормативными документами Организации, которые дополняют и уточняют ее.

**2.Список терминов и определений.**

**Авторизация**-предоставление прав доступа.

**Автоматизированная система**-система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Актив**-все, что имеет ценность для Организации, находится в ее распоряжении.

**Атака на информационную систему**-любое действие, выполняемое нарушителем, которое приводит к реализации угрозы, путем использования уязвимостей системы.

**Защита информации**-основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность мероприятий, необходимых для достижения цели защиты информации и объекта.

**Информационная безопасность**-состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность.

**Информационная система**-совокупность программно-аппаратных комплексов Организации, применяемых для обеспечения бизнес-процессов.

**Нарушитель**-лицо, которое предприняло попытку несанкционированного доступа к ресурсам системы.

**Организация**-ООО «Облако».

**Угроза информационной безопасности**-угроза нарушения свойств информационной безопасности: доступности, целостности или конфиденциальности информационных активов Организации.

**Ущерб**-утрата активов, повреждение активов и инфраструктуры Организации или другой вред, наступивший в результате реализации угроз информационной безопасности через уязвимости информационной безопасности.

**3.Описание объекта защиты**

Основными объектами защиты системы информационной безопасности в Организации

являются информационные ресурсы, содержащие:

* коммерческую тайну;
* персональные данные физических лиц (сотрудников и клиентов);
* сведения ограниченного доступа;
* открыто распространяемую информацию, необходимую для работы Организации,

независимо от формы и вида ее представления.

* платежная информация;
* носители защищаемой информации, в т.ч. информационные ресурсы, речевая информация, документы на физических носителях информации, определенные как защищаемые нормативно-распорядительными документами Организации.

**4.Цели и задачи деятельности по обеспечению информационной безопасности.**

Целью деятельности по обеспечению информационной безопасности Организации является снижение уровня угроз информационной безопасности и защита от ущерба.

Основные задачи деятельности по обеспечению информационной безопасности Организации:

* выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
* исключение либо минимизация выявленных угроз;
* повышение уровня информационной безопасности Организации;
* разработка и поддержание в актуальном состоянии нормативных документов Организации в области информационной безопасности;
* предотвращение инцидентов информационной безопасности и минимизация возможного ущерба от инцидентов;
* внедрение, поддержка и при необходимости восстановление систем защиты информации;
* участие в расследованиях инцидентов информационной безопасности;
* участие и осуществление контроля выполнения требований информационной безопасности в ИТ-проектах Организации;
* согласование и контроль предоставления доступа к информационным активам Организации.

**5.Угрозы информационной безопасности.**

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей. К антропогенным угрозам относятся угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности Организации и контрольных органов, с действиями в руководстве и управлении (менеджменте), неадекватными целям и сложившимся условиям, с потребляемыми услугами, с человеческим фактором.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре Организации могут быть как внешними, так и внутренними.

**6.Основные положения по обеспечению информационной безопасности.**

* Своевременность обнаружения проблем.
* Прогнозируемость развития проблем.
* Оценка влияния проблем.
* Адекватность и эффективность защитных мер.
* Использование опыта при принятии и реализации решений.
* Непрерывность принципов безопасного функционирования.
* Контролируемость защитных мер.
* Назначение ответственных лиц в области информационной безопасности.
* Координация деятельности отдела информационной безопасности.
* Информирование руководства и отдела информационной безопасности о выявленной угрозе в информационной среде.
* Определенность целей (функциональные цели и цели информационной безопасности определены Политикой).
* Назначение и распределение функциональных прав и обязанностей и обеспечение доверия к персоналу Организации.
* Использование ресурсов информационно-телекоммуникационной сети «Интернет».
* Использование средств криптографической защиты информации.
* Проверка подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических данных.
* Контроль отсутствия уязвимостей в оборудовании и программном обеспечении.

**7.Ответственность и контроль соблюдения Политики.**

Ответственность за поддержание положений настоящей Политики и основных нормативных документов Организации в области ИБ лежит на отделе информационной безопасности.

Ответственность сотрудников Организации за неисполнение настоящей Политики и основных нормативных документов в области ИБ определяется соответствующими положениями, включаемыми в договоры с работниками Организации, а также положениями внутренних нормативных документов.

Общий контроль состояния информационной безопасности Организации осуществляет начальник отдела безопасности.

Текущий контроль соблюдения настоящей Политики осуществляет отдел информационной безопасности. Контроль осуществляется путем проведения мониторинга инцидентов информационной безопасности, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

Служба внутреннего аудита осуществляет контроль соблюдения настоящей Политики на основе проведения внутренних проверок информационной безопасности.