|  |  |  |
| --- | --- | --- |
| |  | | --- | | 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»** | |
|  | |
| Выполнил студент группы БИСО-01-19 | Шагалина Алина Денисовна  Аккаунт github: https://github.com/Evzdrafia |
|  |

Москва 2020

Компания ОАО «Кузьма». Штат — 37 сотрудников. 3 руководство, 2

бухгалтерия, 1 — IT-отдел, 19 — менеджеры по работе с клиентами, 3 — отдел информационной

безопасности, 2 – капибары, 2 - отдел охраны, 4 – курьеры, 1 - кипер. Управление компании использует телефонную связь, MS Office, 1С:Предприятие.

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 данных клиентов и компании, а так же секрета производства.

общие положения

Политика информационной безопасности ОАО «Кузьма» разработана в соответствии с законодательством Российской Федерации, доктриной информационной безопасноти РФ (от 09.09.2000), нормами права в части обеспечения ИБ и нормативными документов Организации.

Настоящая Политика является документом, доступным любому сотруднику или клиенту Органиации и обязательным для выполнения сотрудниками, руководством и пользователям его ресурсов.

Организация, как собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения в полном объеме реализует полномочия владения, пользования, распоряжения указанными объектами и определяет условия использования этой продукции.

Организация, как собственник информации, составляющей коммерческую тайну, имеет право передавать и продавать ее другим юридическим и физическим лицам в качестве товара.

Для предотвращения реализации угроз и их последствий документированная информация, информационные системы, технологии и средства их обеспечения подлежат защите.

термины и определения

Актив - все, что имеет ценность для Организации и находится в её распоряжении

Информация – сведения (сообщения, данные) независимо от формы их представления

Информационная безопасность (ИБ) – состояние защищенности интересов (целей) в условиях угроз в информационной сфере.

Оранизация - ОАО «Кузьма»

Политика информационной безопасности – документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Ущерб – утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры Организации или другой вред активам и (или) инфраструктуре Организации, наступивший в результате реализации угроз ИБ через уязвимости ИБ.

Угроза – опасность, предполагающая возможность потерь (ущерба).

Угроза информационной безопасности (угроза ИБ) – угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов Организации.

Уязвимость - слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами

описание объекта защиты

Основными объектами защиты в Организации являются:

− информационные ресурсы, составляющие коммерческую тайну, персональные данные физических лиц, секрет производства и иные чувствительные к нарушению их безопасности информационные ресурсы, представленные в виде документов и массивов информации, независимо от формы и вида их представления (носителя);

− информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал организации;

− информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее передачи, хранения, обработки и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

цели и задачи по обеспечению информационной безопасности

Главной целью обеспечения ИБ является защита информационных активов от случайных (ошибочных) и направленных противоправных посягательств, разглашения, утраты, утечки, искажения, модификации и уничтожения охраняемых сведений.

Основными задачами обеспечения ИБ являются:

− предотвращение утечки, хищения, утраты, искажения, подделки информации;

− предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

− предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;

− защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах.

угрозы информационной безопасности

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные (природные)

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.

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 (природным) 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.

Основные положения по обеспечению информационной безопасности

Обеспечение ИБ при назначении и распределении ролей обеспечения доверия к персоналу:

− при приеме на работу проводится проверка идентичности личности, заявляемой квалификации, точности и полноты биографических фактов, наличия рекомендаций;

− весь персонал дает письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики;

− для внешних организаций требования по ИБ регламентируются положениями, включаемыми в договоры (соглашения).

Защита от несанкционированного доступа и нерегламентированныч действия в рамках предоставленных полномочий в информационных системах обеспечивается посредством:

− предоставления прав доступа к информационным системам на основе действующих ролей, в соответствии с принципом минимально необходимого уровня доступа, т.е. пользователи получают доступ к тем и только тем операциям и данным, которые им необходимы для выполнения своих должностных обязанностей и предусмотрены ролью данного сотрудника;

− предоставление/лишение и изменение прав доступа возможно только после предварительного согласования администратором информационной безопасности, осуществляющим, кроме того, контроль правильности устанавливаемых прав доступа.

Обеспечение ИБ при использовании ресурсов сети Интернет:

− ресурсы сети Интернет используются для получения и распространения информации, связанной с деятельностью Организации, информационноаналитической работы, обмена почтовыми сообщениями исключительно с внешними организациями, а также ведения хозяйственной деятельности Организации. Использование сети Интернет в неустановленных целях запрещается;

− для осуществления безопасного электронного почтового обмена через сеть Интернет применяются защитные меры.

Обеспечение ИБ платежных технологических процессов;

− Организация принимает необходимые организационные и технические меры, для защиты платежной информации.

Обработка персональных данных:

− Организация при обработке персональных данных принимает необходимые организационные и технические меры, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

На основе сформированных требований выбираются меры по обеспечению ИБ

Ответственность и контроль за соблюдением положений Политики

Общее руководство и контроль за обеспечением информационной безопасности осуществляет начальник отдела безопасности

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности Организации лежит на руководстве отдела информационной безопасности.

Ответственность работников Организации за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры с работниками, а также положениями внутренних нормативных документов Организации.

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