НЕОБХОДИМОСТЬ ВНЕДРЕНИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОРГАНИЗАЦИЙ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Исаулова Алла Игоревна

студент, ФГБОУ ВО Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского, РФ, г. Липецк

Золотарева Татьяна Александровна

старший преподаватель кафедры информатики, информационных технологий и защиты информации, ФГБОУ ВО Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского, РФ, г. Липецк

THE NEED TO IMPLEMENT AN INFORMATION SECURITY POLICY FOR ORGANIZATIONS IN THE INFORMATION SOCIETY

Alla Isaulova

Student, Lipetsk State Pedagogical P. Semenov-Tyan-Shansky University, Russia, Lipetsk

Zolotareva Tatyana Aleksandrovna

Senior lecturer of the Department of Informatics, Information Technologies and Information Security, Lipetsk State Pedagogical P. Semenov-Tyan-Shansky University, Russia, Lipetsk

Аннотация. На основании краткого анализа в статье было выявлена значимость и эффективность для организаций и предприятий использование политики информационной безопасности для предотвращения или минимизации утечки информации за пределы организации. В статье рассматриваются основные понятия, принципы решения политики информационной безопасности, которые позволяют минимизировать последствия утечки значимой информации.

Abstract. Based on a brief analysis, the article revealed the importance and effectiveness for organizations and enterprises of using information security policies to prevent or minimize information leakage outside the organization. The article discusses the basic concepts and principles of solving the information security policy, which allow minimizing the consequences of the leakage of significant information.

Ключевые слова: информационные технологии; утечка информации; несанкционированный доступ.

Keywords: information technologies; information leakage; unauthorized access.

Введение. С распространением информационных технологий в нашу жизнедеятельность, мы все чаще и чаще сталкиваемся с проблемой обеспечения информационной безопасности. Как показывает практика, происходит множество инцидентов с кражей особо важной информации на объектах информатизации и организациях, представляющих коммерческую тайну, и все чаще причиной утечки информации остается в пренебрежительном отношении или не соблюдение методов и стандартов, которые позволяют обеспечить защиту информации. Поэтому так необходимо всем предприятиям, которые имеют отношение к особо важным данным обеспечивать защиту своих систем от взлома, изменения, редактирования, копирования или уничтожения особо важной информации. Однако же не многие понимают насколько важна разработка политики информационной безопасности и тем более не знают, как правильно разработать конкретно для своего предприятия политику, для комплексной и эффективной защиты. Поэтому в данной статье мы рассмотрим основные аспекты политики информационной безопасности и разберемся, как правильно ее составлять и использовать.

Определение политики информационной безопасности. Прежде чем говорить о важности и основных методов обеспечения политики информационной безопасности необходимо понять, что она из себя представляет. Если говорить о политики информационной безопасности (далее - Политика) в целом, то это совокупность требований, стандартов, рекомендаций и регламентов, согласно которым ведется профессиональная деятельность компании, предприятия или организации, чтобы обеспечить защиту информационных ресурсов и систем, расположенных на ее территории.

Если же говорить о назначении и правовой основе, то настоящая политика информационной безопасности разработана на основе требований Российской Федерации нормативных и законодательных документов, которые регламентируют вопросы защиты информации Организации, она учитывает цели, задачи и правовые основы создания, эксплуатации и функционирования информационных систем Организации.

Положения и требования политики информационной безопасности распространяется на все предприятия и учреждения, входящие в состав Организации, а также на основных разработчиков и исполнителей, которые участвуют в разработке, создании и вводе в эксплуатацию информационной системы.

Политика информационной безопасности базируется на методологической основе и служит для:

- разработки подсистемы информационной безопасности, реализуемой на объектах информатизации с ограниченным доступом, в виде комплексной системы защиты информации от несанкционированного доступа;
- разработки защищенного электронного документооборота, с использованием средств защиты информации, а также применения электронной цифровой подписи и частных виртуальных сетей обмена защищаемой информации;
- разработки нормативных документов и мероприятий, для обеспечения информационной безопасности;
- реализации определенных прав лицам, организациям на получение, распространение и использование информации.

Если же говорить о основных принципах политики, то она основывается на:

- соблюдение Конституции Российской Федерации, законов Российской Федерации;
- достижение целей и задач, поставленных в уставном положении Организации;
- оценка состояния информационной безопасности, выявление источников угроз информационной безопасности, определение приоритетных направлений предотвращения, минимизации и нейтрализации этих угроз;
- применение сертифицированных средств защиты информации и лицензирование деятельности в области защиты информации;
- совершенствование и развитие системы подготовки кадров в области информационной безопасности.[1]

Разработка Политики. Прежде всего, перед тем как внедрить Политику руководителю

Организации важно понимать, что она необходима для того, чтобы донести до бизнеса основные цели и задачи информационной безопасности компании. А сама политика требуется для обоснования введения защитных мер в Организации, которая должна быть утверждена высшим административным органом предприятия.

Как показывает практика, чаще всего несанкционированный доступ к важной информации и последующая ее утечка за пределы Организации происходит по вине пользователя, потому что ему он относится к этому пренебрежительно, но при наличии в компании политики информационной безопасности, такого не происходит и пользователь вынужден соблюдать установленные Организацией предписанные требования, чтобы не нести за это ответственность перед компанией.

Разработка политики информационной безопасности. При разработке политики информационной безопасности необходимо помнить, что:

- целевая аудитория политики - это конечные пользователи, которые не всегда понимают сложные термины и определения, но которые необходимо ознакомится с положениями политики.
- Необходимо включать только цели, задачи, методы и ответственность. Не нужно включать сложных технических подробностей, т.к. они могут быть непонятны пользователю.

По окончанию составления документ должен удовлетворять следующим требованиям:

- лаконичность — не нужно писать огромные документы иначе конечный пользователь просто не станет читать такой объем и как следствие, не будет соблюдать ваш регламент.
- доступность — как говорилось ранее, пользователь должен понимать, что написано в документе, чтобы правильно выполнять необходимые требования.

Внедрение и использование. После того как будет разработан и утвержден документ необходимо:

- ознакомить с политикой сотрудников Организации, это касается как новых, так и уже работающих на предприятии работников;
- провести анализ бизнес-процесса для выявления и минимизации рисков;
- разработать инструкции и положения, дополняющие Политику;
- производить пересмотр Политики с целью актуализации.

Выводы. Итак, подведем итоги всему вышесказанному. Политика информационной безопасности является эффективным и надежным документов для реализации защиты данных от несанкционированного доступа к информации, а также ее копированию, распространению или изменению. Благодаря Политики, Организация может минимизировать риски утечки информации и более доступно объяснить своим пользователям необходимость соблюдения правил безопасности.

Список литературы:

1. Свободное общество dataved.ru: Политика информационной безопасности Организации [Электронный ресурс]. – Режим доступа: http://www.dataved.ru/2010/03/information-security.html#base (дата обращения: 25.06.2021)

2. Политика информационной безопасности [Электронный ресурс]. – Режим доступа:https://zen.yandex.ru/media/cisoclub/politika-informacionnoi-bezopasnosti-5f7188eafde6297ce3225112#:~:text=Политика%20информационной%20безопасности%20–%20совокупность,имеющихся%20у%20нее%20информационных%20ресурсов (дата обращения: 25.06.2021)

3. Политика информационной безопасности — опыт разработки и рекомендации/Хабр

[Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/174489/ (дата обращения: 25.06.2021)