УДК 004.056

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧРЕЖДЕНИЯХ СИСТЕМЫ ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Петров А.Д.

гр.367241

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Петров С.Н. – кандидат технических наук, доцент кафедры защиты информации

Аннотация. В материалах доклада рассматривается методика разработки политики информационной безопасности в учреждениях системы высшего образования Республики Беларусь с учетом требований Приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. №66.

Ключевые слова: политика информационной безопасности, информационная безопасность

Введение. Политика информационной безопасности играет ключевую роль в обеспечении защиты информационных активов организации. Она позволяет определить основные направления и приоритеты в области информационной безопасности, установить ответственность и обязанности сотрудников.

Политика информационной безопасности позволяет разработать эффективные меры по предотвращению, обнаружению и реагированию на угрозы информационной безопасности

Руководящие документы оказывают значительное влияние на содержание политики информационной безопасности. Они определяют требования и стандарты, которым должна соответствовать система информационной безопасности организации. Указ Президента Республики Беларусь №449 от 9 декабря 2019 года «О совершенствовании государственного регулирования в области защиты информации» [1] является примером такого документа и устанавливает ряд требований и принципов для обеспечения безопасности информационных систем и обработки информации. О мерах по реализации Указа Президента Республики

Беларусь от 9 декабря 2019 года №449 подробно описано в Приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. №66 [2].

Основная часть. Согласно пункта 9 главы 2 положения о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено политика информационной безопасности организаций должна содержать:

– цели и принципы защиты информации в организации;

– перечень информационных систем, отнесенных к соответствующим классам типовых информационных систем, а также отдельно стоящих электронных вычислительных машин, используемых в организации и принадлежащих ей на праве собственности или ином законном основании, с указанием подразделения защиты информации или иного подразделения (должностного лица), ответственного за обеспечение защиты информации;

– обязанности пользователей информационной системы;

– порядок взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия), в том числе при осуществлении информационных отношений на правах операторов, посредников, пользователей информационных систем и обладателей информации.

Основными целями политики информационной безопасности учреждений системы высшего образования являются:

– сохранение конфиденциальности критичных информационных ресурсов;

– обеспечение непрерывности доступа к информационным ресурсам учреждений системы высшего образования;

– защита целостности информации с целью поддержания возможности учреждений системы высшего образования по оказанию услуг высокого качества и принятию эффективных управленческих решений;

– повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами учреждений системы высшего образования;

– определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности;

– предотвращение и/или снижение ущерба от инцидентов информационной безопасности.

Основными задачами политики информационной безопасности учреждений системы высшего образования являются:

– разработка требований по обеспечению информационной безопасности;

– контроль выполнения установленных требований по обеспечению информационной безопасности;

– повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;

– разработка нормативных документов для обеспечения информационной безопасности учреждений информационной безопасности;

– выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности учреждений высшего образования;

– организация антивирусной защиты информационных ресурсов учреждений системы высшего образования;

– защита информации учреждений системы высшего образования от несанкционированного доступа и утечки по техническим каналам связи;

– организация периодической проверки соблюдения информационной

безопасности с последующим представлением отчета по результатам указанной проверки ректору учреждения высшего образования.

Политика информационной безопасности образовательных учреждений направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшения рисков и снижения потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников образовательного учреждения, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора, хранения, обработки, предоставления и распространения информации и обеспечение и бесперебойного процесса деятельности.

Наибольшими возможностями для нанесения ущерба обладает собственный персонал учреждений системы высшего образования.

Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

Стратегия обеспечения информационной безопасности высших образовательных учреждений заключается в использовании заранее отработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму потери от технических аварий и ошибочных действий сотрудников высших учебных учреждений.

Основными принципами обеспечения информационной безопасности:

– постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов учреждений высшего образования;

– своевременное обнаружение проблем, корректировка моделей угроз и нарушителя;

– персонификация и разделение ролей и ответственности между сотрудниками.

Объектами защиты с точки зрения информационной безопасности являются:

– информационный процесс профессиональной деятельности;

– информационные активы учреждений высшего образования.

Защищаемая информация делится на следующие виды:

– информация по финансово-экономической деятельности учреждений высшего образования;

– персональные данные – личные сведения о человеке, с помощью которых его можно идентифицировать согласно Закона Республики Беларусь от 7 мая 2021 года №99-З «О защите персональных данных»;

– другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования».

Управление информационной безопасностью учреждений системы высшего образования включает в себя:

– разработку и поддержание в актуальном состоянии Политики информационной безопасности;

– разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению информационной безопасности;

– обеспечение бесперебойного функционирования комплекса средств информационной безопасности;

– осуществление контроля (мониторинга) функционирования системы информационной безопасности;

– оценку рисков, связанных с нарушения информационной безопасности.

Заключение. Политика информационной безопасности является основным документом организации по обеспечению и организации информационной безопасности. Соблюдение требований политики информационной безопасности позволяет минимизировать риски и угрозы информационной безопасности в процессе обучения абитуриентов и работы сотрудников учреждений высшего образования.

Список литературы

1. Указ Президента Республики Беларусь от 9 декабря 2019 года № 449 «О совершенствовании государственного регулирования в области защиты информации» – Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by

2. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 года № 449» – Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by

UDC 004.056

INFORMATION SECURITY POLICY IN INSTITUTIONS OF THE HIGHER EDUCATION SYSTEM OF THE REPUBLIC OF BELARUS

Petrov A.D.

gr.367241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Petrov S.N. – PhD, associate professor of the Information Security Department

Annotation. The materials of the report discuss the methodology for developing an information security policy in institutions of the higher education system of the Republic of Belarus, taking into account the requirements of the Order of the Operational Analytical Center under the President of the Republic of Belarus dated February 20, 2020 No. 66

Keywords: information security policy, information security.