Зайцева Е.С.
Научный руководитель: к.т.н., инженер вычислительного центра А. В. Астафьев
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail: katlabutova@yandex.ru

Реализация групповой политики безопасности

В системе должна быть единая политика безопасности, которая определяет правила обращения с информацией так, чтобы исключить или снизить угрозы ущерба. Единая политика нужна, чтобы исключить противоречия между правилами обращения с одной и той же информацией в разных подразделениях организации. В самом простом случае, это дискреционная политика. При такой политике у каждого информационного объекта системы есть хозяин, который определяет правила доступа субъектов к объектам. Для реализации дискреционной политики безопасности каждый субъект и объект должны быть идентифицированы, а каждый субъект должен подтвердить свой идентификатор (аутентификация) [1]. Обычно дискреционную политику безопасности усиливают аудитом, отслеживая активность пользователей или субъектов, которые действуют от их имени, в компьютерной системе. Исходя из этого реализация групповой политики безопасности информационной системы является актуальной научно-технической задачей.

Целью исследования является реализация групповой политики безопасности.

Кроме дискреционной политики безопасности как минимум необходимо организовать защиту целостности информационных ресурсов от модификации или уничтожения. Идентификация и аутентификация, правила разграничения доступа, аудит и защита целостности должны реализовываться механизмами защиты. На каждом рабочем месте и на серверах установлены операционные системы, которые, как правило, обладают набором механизмов защиты, обеспечивающих идентификацию и аутентификацию, разграничение доступа, аудит на данном компьютере. Серьезные прикладные системы типа СУБД также обладают локальным набором механизмов защиты, обеспечивающих идентификацию и аутентификацию, разграничение доступа и аудит. Основными механизмами защиты целостности являются резервное копирование (backup), электронно-цифровая подпись (ЭЦП) и коды аутентификации [3].

Сравним эти механизмы:

Название	Криптостойкость	Целостность	Разграничение доступа
Резервное копирование	-	+	-
ЭЦП	+	+	+
Коды аунтефикации	-	+	+

В ходе исследования можно увидеть на основе сравнения механизмов защиты, наиболее надежной защитой информации и данных является ЭЦП, так как у нее больше преимуществ перед другими механизмами защиты.

Литература

1. Кияев В., Граничин О. «Безопасность информационных систем: курс». 2016 г.
2. Скрипник Д. А. «Общие вопросы технической защиты информации», 2016 г.
3. Блинов А. М. «Информационная безопасность», 2010 г.