ISSN 2658 – 7505
Выпуск №2, 2019
Электронный научный журнал «Вестник молодёжной науки России»

УДК 004.056.53

АНАЛИЗ РАСПРЕДЕЛЕНИЯ ПРАВ ДОСТУПА

***М.Н. Кононов, П.К. Коробейникова, Н.Б. Кононов, Н.В. Кононова**, e-mail: knv_fm@mail.ru*
ФГАОУ ВО Северо-Кавказский федеральный университет (СКФУ), г. Ставрополь

В данной статье рассматриваются меры информационной безопасности при функционировании корпоративной автоматизированной системы управления, предлагаются реальные предпосылки к возможности проведения атак, направленных на разрушение телекоммуникационной инфраструктуры, используемой предприятием, а также утечки по техническим каналам и при помощи несанкционированного доступа к конфиденциальной информации, циркулирующей в ней. Одним из самых уязвимых мест в защите, является распределение прав доступа. В политике безопасности должна быть утверждена схема управления распределением прав доступа к сервисам – централизованная и децентрализованная. Должно быть четко определено, кто распоряжается правами доступа к сервисам и какими именно правами.

Ключевые слова: политика безопасности, система информационной безопасности, права доступа к сервисам

ANALYSIS OF THE DISTRIBUTION OF ACCESS RIGHTS

***M.N. Kononov, P.K. Korobeynikov, N.B. Kononov, N.V. Kononova**, e-mail: knv_fm@mail.ru*
FSAEI North-Caucasus Federal University (NCFU), Stavropol

This article discusses information security measures in the operation of the corporate automated management system, offers real prerequisites for the possibility of attacks aimed at destroying the telecommunications infrastructure used by the enterprise, as well as leaks through technical channels and through unauthorized access to confidential information circulating in it. One of the most vulnerable places to protect is the allocation of access rights.The security policy must approve a scheme for managing the allocation of access rights to services - centralized and decentralized. It should be clearly defined who disposes of the rights of access to the services and which rights.

Keywords: security policy, information security system, access rights to services

В настоящее время информационный ресурс стал одним из наиболее мощных рычагов экономического развития. На данный момент трудно представить себе фирму или предприятие, у которых отсутствовали бы современные средства обработки и передачи информации. Наличие разного рода информации порождает целый ряд сложных и крупномасштабных проблем. Одной из таких проблем является надежное обеспечение сохранности и доступности информации, циркулирующей и обрабатываемой в распределенных информационных системах.

Прежде чем внедрять какие – либо решения по защите информации, необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Система информационной безопасности окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности, проведение анализа риска и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности. Политика безопасности должна существовать в виде отдельного документа и утверждаться руководством предприятия [1].

Политика безопасности является необходимым элементом построения эффективной системы обеспечения информационной безопасности. Ее главное предназначение – защита сотрудников и информационных активов компании. Политика минимизирует влияние «человеческого фактора» и недостатки существующих технологий, позволяет вовлечь сотрудников в процесс обеспечения информационной безопасности, является эффективным и дешевым решением создания культуры безопасности в компании.

Таким образом, тема актуальна и требует комплексного подхода к формированию политики информационной безопасности корпоративной автоматизированной системы управления на основе руководящих документов ФСТЭК.

Регламентирующих состав и функциональные характеристики средств защиты информации в корпоративных автоматизированных системах управления, необходимых для обеспечения надежной защиты политики информационной безопасности и разработки автоматизированных систем, обрабатывающих персональные данные, а также информацию, составляющую технологическую, коммерческую тайну предприятия и политику информационной безопасности.

Одним из самых уязвимых мест в защите является распределение прав доступа. В политике безопасности должна быть утверждена схема управления распределением прав доступа к сервисам – централизованная и децентрализованная. Должно быть четко определено, кто распоряжается правами доступа к сервисам и какими именно правами.

Права и обязанности пользователей определяются применительно к безопасному использованию подсистем и сервисов корпоративной автоматизированной системы управления. При определении прав администраторам и специалистам по информационной безопасности следует стремиться к некоторому балансу между правом пользователей на тайну и их обязанностями контролировать нарушения.

Важным элементом политики информационной безопасности является распределение ответственности. При ее разработке невозможно предусмотреть всего.

Обычно выделяются несколько уровней ответственности. На первом уровне каждый пользователь обязан работать в соответствии с политикой информационной безопасности (защищать свой счет). Подчиняться распоряжениям должностных лиц, отвечающих за отдельные аспекты безопасности. Системные администраторы отвечают за защиту информационно–вычислительных подсистем. Специалисты по информационной безопасности должны обеспечивать реализацию организационно–технических мер, необходимых для безопасности корпоративной автоматизированной системы управления. Руководители подразделений отвечают за доведение и контроль положений политики безопасности [2].

С практической точки зрения, политику информационной безопасности целесообразно разделить на несколько уровней, основное внимание необходимо уделить порядку создания и пересмотра политики информационной безопасности, целям, преследуемым предприятием в области информационной безопасности, вопросам выделения и распределения ресурсов, принципам технической политики в области выбора методов и средств защиты информации, координированию мер безопасности, стратегическому планированию и контролю, внешним взаимодействиям и другим вопросам, имеющим общеорганизационный характер.

Средний уровень политики информационной безопасности выделяют в случае структурной сложности предприятия. Это касается отношения к перспективным технологиям. Кроме того, на среднем уровне политики информационной

безопасности могут быть выделены особо значимые контуры корпоративной автоматизированной системы управления.

За разработку и реализацию политики информационной безопасности верхнего и среднего уровней отвечают руководитель службы безопасности, специалисты по информационной безопасности корпоративной автоматизированной системы управления, администратор корпоративной сети.

Нижний уровень политики информационной безопасности относится к конкретным службам или подразделениям предприятия. Данный уровень необходим, когда вопросы безопасности конкретных подсистем требуют решения на управленческом, а не только на техническом уровне.

Понятно, что на данном уровне определяются конкретные цели, частные критерии и показатели информационной безопасности, определяются права конкретных групп пользователей, формулируются соответствующие условия доступа к информации. Здесь из конкретных целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать или не может.

На этом уровне описываются механизмы защиты информации и используемые программно-технические средства для их реализации (в рамках, конечно, управленческого уровня, но не технического) [2].

Политика информационной безопасности — это важный атрибут любой организации независимо от ее размера. Неважно большая или маленькая компания в ней должна быть политика безопасности и часть этой политики посвящена информационной безопасности. Необходимо разрабатывать методики формирования политики информационной безопасности. При создании политики информационной безопасности необходимо решать задачи по достижению защищенной инфраструктуры для обеспечения защищенного документооборота и обработки персональных данных. Решение данных задач позволит сохранить активы компании. Необходимо производить анализ методики управления рисками при определении политики информационной безопасности корпоративной автоматизированной системы управления, где важной частью процесса управления информационной безопасностью является оценка уровня рисков и методов снижения его до приемлемого уровня.

Список цитируемой литературы

1. Российская Федерация. Конституция (1993). Конституция Российской Федерации: офиц. текст. – М.: Маркетинг, 2001. – 39 с.
2. Чипига А.Ф. Информационная безопасность автоматизированных систем, 2010. – 336 с.