УДК 004.056

Шишкин Н.Д.,
старший инженер отдела кибербезопасности ПАО «Сбербанк»
Россия, г. Барнаул

АВТОМАТИЗАЦИЯ ПРОЦЕССА УСТАНОВКИ И НАСТРОЙКИ АНТИВИРУСНОЙ ЗАЩИТЫ В КОРПОРАТИВНОЙ СЕТИ НА БАЗЕ KASPERSKY SECURITY CENTER

Аннотация. *Аннотация. В статье рассматривается практическая реализация системы централизованного управления антивирусной защитой на примере программного комплекса Kaspersky Security Center (КСЦ). Анализируются современные угрозы информационной безопасности, обосновывается необходимость применения криптографических и организационных мер защиты. Особое внимание уделяется сравнительному анализу ручного и автоматизированного способов установки агента администрирования и антивирусного ПО, демонстрируется эффективность использования серверной инфраструктуры для обеспечения безопасности корпоративной сети. Приведены практические рекомендации по настройке задач и политик безопасности.*

Ключевые слова: *информационная безопасность, антивирусная защита, Kaspersky Security Center, централизованное управление, установка ПО, модель угроз, корпоративная сеть.*

Annotation: *The article discusses the practical implementation of a centralized antivirus protection management system using the Kaspersky Security Center (KSC) software package as an example. Modern threats to information security are analyzed, and the need for cryptographic and organizational protection measures is justified. Special attention is paid to the comparative analysis of manual and automated methods of installing the administration agent and antivirus*

software, demonstrating the effectiveness of using the server infrastructure to ensure the security of the corporate network. Practical recommendations on configuring tasks and security policies are provided.

Key words: *information security, antivirus protection, Kaspersky Security Center, centralized management, software installation, threat model, corporate network.*

Развитие информационных технологий неразрывно связано с появлением новых вызовов в сфере защиты данных. Информация, являясь ключевым ресурсом современного общества, требует комплексной защиты от несанкционированного доступа, модификации и уничтожения. Законодательная база Российской Федерации, в частности Доктрина информационной безопасности, обязывает организации внедрять необходимые меры защиты, включая использование сертифицированных средств криптографической защиты информации (СКЗИ) и антивирусных программ. Однако, как показывает практика, отсутствие централизованного управления защитой на предприятии приводит к снижению общего уровня безопасности из-за человеческого фактора, сбоев в обновлении баз и фрагментарной установке ПО.

Актуальность исследования обусловлена необходимостью разработки эффективных методов развертывания систем защиты в условиях ограниченного бюджета и возрастающего числа киберугроз. Целью данной работы является анализ и практическая демонстрация настройки антивирусного программного обеспечения «Лаборатории Касперского» с использованием консоли администрирования Kaspersky Security Center (КСЦ) для повышения надежности и управляемости системой информационной безопасности предприятия.

Прежде чем переходить к практическим решениям, необходимо определить базовые понятия. Информационная безопасность (ИБ)

представляет собой состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий, результатом которых может стать ущерб субъектам информационных отношений. Ключевыми свойствами информации являются конфиденциальность (доступность только для авторизованных лиц), целостность (неискаженность) и доступность (возможность своевременного получения).

Анализ защищаемой информации требует ее структурирования по содержанию. В теории ИБ выделяют семантическую информацию (смысловое содержание) и признаковую (описывающую физические свойства объектов). Для обеспечения сохранности этих данных применяются различные методы, среди которых ключевое место занимает криптография. Криптографические методы защиты информации включают шифрование (преобразование данных без изменения объема) и кодирование (сжатие или замена сочетаний символов). Однако эффективность шифрования напрямую зависит от управления криптографическими ключами — сменных элементов шифра, которые должны быть защищены от компрометации.

В рамках построения системы защиты критически важно описать модель угроз и модель нарушителя. Угрозы могут быть пассивными (направленными на несанкционированное использование информации без влияния на работу системы, например, прослушивание) и активными (целенаправленное нарушение функционирования ИС с помощью вирусов, отказ в обслуживании). Особую опасность представляют внутренние нарушители (сотрудники, администраторы, персонал) и внешние (конкуренты, хакеры). Мотивами действий могут быть как корыстные интересы, так и ошибки или некомпетентность. Для противодействия данным угрозам, помимо организационных мер, применяются специализированные программные продукты, такие как Dallas Lock, ViPNet CSP и антивирусные пакеты. Эволюция антивирусных продуктов, в частности история создания

«Лаборатории Касперского», начавшаяся с вируса Cascade в 1989 году, показывает необходимость постоянной адаптации защиты к новым типам вредоносного ПО.

Эффективность антивирусной защиты в масштабах предприятия достигается внедрением системы централизованного управления. В качестве такого инструмента в работе используется Kaspersky Security Center (КСЦ) — программное решение, позволяющее администраторам управлять политиками безопасности, обновлениями и установкой ПО на всех рабочих станциях и серверах сети.

Управление инфраструктурой. Работа с КСЦ происходит через удаленное подключение к серверу (по RDP), где размещена консоль администрирования. Основным рабочим полем является дерево групп управляемых устройств. Данная иерархия позволяет гибко распределять задачи: некоторые из них наследуются всеми устройствами (например, глобальное обновление антивирусных баз или плановая проверка), тогда как для конкретных подразделений (в примере — группа «kgkh») могут создаваться уникальные задачи, например, установка специфического лицензионного ключа. Создание задачи осуществляется через мастер задач, где администратор выбирает тип операции (установка, обновление, проверка), задает параметры и область применения.

Методы установки и развертывания. Практическое исследование показало наличие двух основных способов инсталляции антивирусного программного обеспечения на компьютеры пользователей:

1. Ручная установка. Требует физического или удаленного присутствия администратора на рабочей станции. Процесс включает запуск дистрибутива (например, setup.exe для Kaspersky Endpoint Security 11), распаковку и следование шагам мастера установки. Данный метод трудоемок при масштабировании на сотни машин и подвержен ошибкам пользователя.

2. Автоматизированная установка (через КСЦ). Более предпочтительный метод для корпоративных сетей. В консоли администрирования создается автоматическая задача для агента администрирования и самого антивируса. Когда новое устройство появляется в сегменте сети, оно попадает в раздел «Нераспределенные устройства». Администратор перемещает его в нужную группу, после чего сервер автоматически инициирует удаленную установку необходимого ПО (Remote Installation). Этот способ обеспечивает единообразие конфигураций и существенно сокращает время развертывания.

Контроль успешности установки осуществляется через стандартный апплет Windows «Программы и компоненты», где должны отображаться установленные компоненты: «Агент администрирования» и «Kaspersky Endpoint Security». Наличие этих записей свидетельствует о полной защите рабочей станции.

В ходе работы были изучены теоретические основы информационной безопасности, включая классификацию угроз, модели нарушителей и криптографические методы защиты. Практическая часть показала, что использование Kaspersky Security Center позволяет вывести антивирусную защиту на качественно новый уровень, обеспечивая централизованный контроль и автоматизацию рутинных операций.

Установка агента и антивируса с использованием серверной консоли администрирования доказала свою эффективность по сравнению с ручным методом, особенно в условиях крупных предприятий. Единственным ограничением, отмеченным в работе, является платный характер лицензирования, однако, по оценкам специалистов, высокая надежность, регулярные обновления и комплексный подход к защите делают продукты «Лаборатории Касперского» экономически целесообразными. Предложенная схема настройки позволяет минимизировать риск заражения сетей и

обеспечивает соблюдение требований законодательства в области защиты персональных данных.

Использованные источники:

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).
2. Запечников С.В., Милославская Н.Г., Толстой А.И. Информационная безопасность открытых систем. — М.: ГЛТ, 2006. Т.1. — 536 с.
3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учебное пособие. — М.: Риор, 2017. — 476 с.
4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. — М.: ГЛТ, 2004. — 280 с.
5. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие. — М.: Форум, 2018. — 432 с.
6. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. — М.: ИД ФОРУМ, 2013. — 416 с.
7. Официальная документация «Лаборатории Касперского» по Kaspersky Security Center. — Режим доступа: support.kaspersky.ru (дата обращения: 10.07.2026).