УДК 004.056
DOI 10.21685/2587-7704-2018-3-2-7

Open Access | RESEARCH ARTICLE

Процесс контроля за состоянием антивирусной защиты

П. А. Гуренков
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

О. В. Липилин
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Рассматривается процесс контроля за состоянием антивирусной защиты. На основе анализа угроз и уязвимостей, связанных с внедрением вредоносного кода, приводится декомпозиция процесса контроля за состоянием антивирусной защиты.

Ключевые слова: вредоносное программное обеспечение, угроза, уязвимость, процесс, управление антивирусной безопасностью.

Monitoring the status of antivirus protection service

P. A. Gurenkov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

O. V. Lipilin
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The monitoring process of antivirus protection status is considered. Its decomposition, based on the analysis of threats and vulnerabilities associated with the introduction of malicious code, is provided.

Keywords: malware, threat, vulnerability, process, antivirus security management.

Актуальными угрозами для большинства информационно-телекоммуникационных систем являются угрозы, связанные с внедрением вредоносного кода. Согласно статистике Лаборатории Касперского [1], представленной на рис. 1, за последние два года количество ежеквартально выявленного вредоносного программного обеспечения (ВПО) стабильно составляет примерно 1,5 млн. Большое количество вирусных атак направлено на различные организации.

Банк данных угроз [2] содержит перечень угроз, связанных с вредоносным программным обеспечением:

– УБИ.006 – угроза внедрения кода или данных, заключающаяся в возможности внедрения нарушителем в дискредитируемую информационную систему вредоносного кода, который может быть в дальнейшем запущен пользователями автоматически при выполнении определенного условия;

– УБИ.167 – угроза заражения компьютера при посещении неблагонадежных сайтов, заключающаяся в возможности нарушения безопасности защищаемой информации вредоносными программами, скрытно устанавливаемыми при посещении пользователями системы с рабочих мест;

– УБИ.170 – угроза неправомерного шифрования информации, заключающаяся в возможности фактической потери доступности защищаемых данных из-за их несанкционированного криптографического преобразования нарушителем с помощью известного только ему секретного ключа;

– УБИ.186 – угроза внедрения вредоносного кода через рекламу, сервисы и контент, заключающаяся в возможности внедрения в информационную систему вредоносного кода посредством ре-

кламы, сервисов или убеждения пользователя системы активировать ссылку при посещении пользователями веб-сайтов с рабочих мест;

– УБИ.189 – угроза маскирования действий вредоносного кода, заключающаяся в возможности сокрытия в системе действий вредоносного кода за счет применения специальных механизмов маскирования кода;

– УБИ.190 – угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет, заключающаяся в возможности осуществления нарушителем внедрения вредоносного кода в компьютер пользователя посредством взлома и заражения часто посещаемых пользователем вебсайтов;

– УБИ.191 – угроза внедрения вредоносного кода в дистрибутив программного обеспечения, заключающаяся в возможности осуществления заражения системы путем установки дистрибутива, в который внедрен вредоносный код;

– УБИ.195 – угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы, заключающаяся в возможности удаленного запуска вредоносного кода за счет создания приложений, использующих обход механизмов защиты, встроенных в операционную систему;

– УБИ.198 – угроза скрытной регистрации вредоносной программой учетных записей администраторов, заключающаяся в возможности скрытного создания внедренной вредоносной программой учетных записей с правами администратора;

– УБИ.208 – угроза нецелевого использования вычислительных ресурсов средства вычислительной техники, заключающаяся в возможности использования вычислительных ресурсов средств вычислительной техники для осуществления сторонних вычислительных процессов.

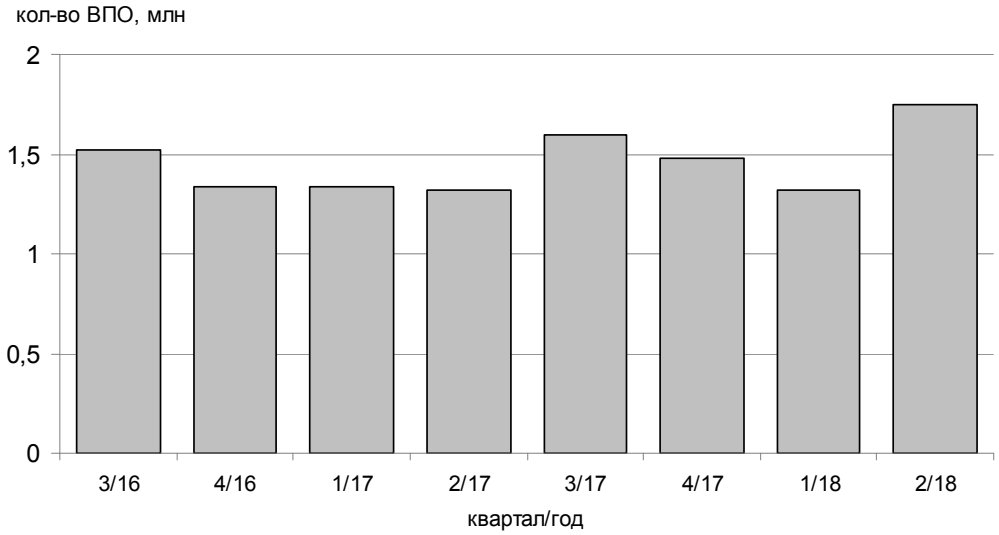

Рис. 1. Количество выявленного вредоносного программного обеспечения

По описанию угроз были определены основные уязвимости, через которые реализуются угрозы. Перечень уязвимостей с указанием индексов угроз приведен в табл. 1.

Таблица 1

Перечень уязвимостей

Уязвимость	Связанные угрозы
1. Уязвимости программного обеспечения	УБИ.006,
2. Уязвимости операционных систем	УБИ.195
3. Слабость мер антивирусной защиты на рабочем месте	УБИ.006, УБИ.170, УБИ.189, УБИ.190, УБИ.191, УБИ.196, УБИ.198, УБИ.208
4. Слабость антивирусного контроля на уровне организации	УБИ.167, УБИ.186, УБИ.190
5. Слабость мер фильтрации сетевого трафика	УБИ.167, УБИ.186, УБИ.190
6. Слабость механизмов разграничения доступа	УБИ.006, УБИ.167, УБИ.170

Из таблицы видно, что через уязвимости 2 и 3, связанные непосредственно с антивирусными средствами, реализуются практически все перечисленные угрозы информационной безопасности. Рассмотрим их подробнее.

Уязвимость «Слабость мер антивирусной защиты на рабочем месте» подразумевает следующее:

– отсутствие или непериодическое обновление антивирусных баз, содержащих сигнатуры вредоносного программного обеспечения;

– неправильная настройка или полное отключение компонентов защиты антивирусных средств;

– использование устаревших версий антивирусных средств;

– отсутствие автоматической проверки устанавливаемого программного обеспечения на наличие вредоносного кода;

– отсутствие автоматического контроля запускаемого программного обеспечения.

Очевидно, что снижение вероятности реализации угроз достигается путем устранения вышеописанных недостатков системы защиты. Однако стоит отметить, что при большом размере организации администратор информационной безопасности (ИБ) не может контролировать состояние антивирусной защиты на каждом рабочем месте. Поэтому для организаций важным является устранение уязвимости «Слабость антивирусного контроля на уровне организации».

Контроль за состоянием антивирусной защиты должен реализовываться в виде непрерывного процесса. Декомпозиция процесса представлена на рис. 2.

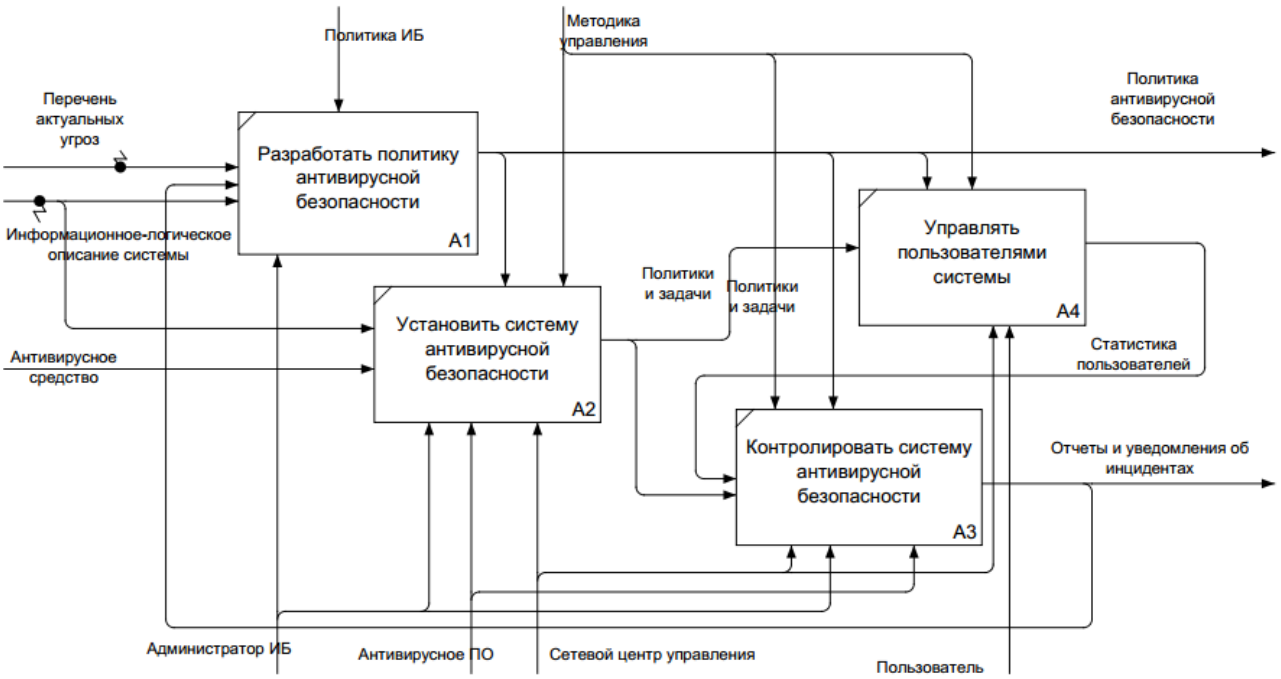

Рис. 2. Декомпозиция процесса «Контроль за состоянием антивирусной защиты»

Таким образом, непрерывное выполнение процесса контроля за состоянием антивирусной защиты позволит снизить вероятность возникновения угроз информационной безопасности, связанных с внедрением в информационно-телекоммуникационную систему вредоносного программного обеспечения.

Библиографический список

1. Статистика – Securelist – Аналитика и отчеты о киберугрозах «Лаборатории Касперского». – URL: https://securelist.ru/all/?category=726, свободный (дата обращения: 30.09.2018).
2. Банк данных угроз безопасности информации. – URL: https://bdu.fstec.ru/threat, свободный (дата обращения: 30.09.2018).

Гуренков, П. А.

Процесс контроля за состоянием антивирусной защиты / П. А. Гуренков, О. В. Липилин // Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-7.