Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования». ТКП устанавливает требования по обеспечению безопасности КВОИ.

Порядок обеспечения безопасности КВОИ, который включает в себя: отнесение ОИ к КВОИ в соответствии с перечнем отраслевых критериев; классификацию КВОИ; реализацию комплекса мероприятий по созданию системы безопасности КВОИ.

Обязанности по обеспечению безопасного функционирования КВОИ возлагаются на его владельца. Классификация КВОИ проводится в соответствии с СТБ 34.101.52-2016 «Информационные технологии. Методы и средства безопасности. Критически важные объекты информатизации. Классификация» (вступил в силу с 01.04.2017).

ИЗМЕНЕНИЕ СТБ 34.101.8-2006 «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. МЕТОДЫ И СРЕДСТВА БЕЗОПАСНОСТИ. ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ И АНТИВИРУСНЫЕ ПРОГРАММНЫЕ СРЕДСТВА. ОБЩИЕ ТРЕБОВАНИЯ

Д.И. ЖУКОВА, О.Ю. КОНДРАХИН, Д.В. ШУЛЯК

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»

С 1 января 2014 г. введен в действие технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утвержденный постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375 (далее - регламент).

Соответствие средств защиты информации (СЗИ) требованиям регламента обеспечивается либо выполнением требований, непосредственно приведенных в регламенте, либо выполнением требований взаимосвязанных с ним нормативно-правовых актов, перечисленных в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2013 г. № 94 «О перечне технических нормативных правовых актов, взаимосвязанных с техническим регламентом ТР 2013/027/BY».

Согласно указанному Приказу программные средства защиты от воздействия вредоносных программ и антивирусные программные средства, выпускаемые в обращение на рынке должны выполнять требования СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования» (далее – стандарт) (пункты 6.2, и (или) 6.3, и (или) 6.4).

В стандарте устанавливаются три типа программных средств защиты от воздействия вредоносных программ и антивирусных программных средств (ПСЗВВП и АПС).

ПСЗВВП и АПС первого типа после запуска по запросу пользователя должны обнаруживать изменения элементов объектов информационных технологий;

ПСЗВВП и АПС второго типа после запуска по запросу пользователя должны обеспечивать проверку элементов объекта информационных технологий на наличие вредоносных программ (ВП) и обезвреживание обнаруженных ВП;

ПСЗВВП и АПС третьего типа в течение работы объекта информационных технологий должны обеспечивать в реальном масштабе времени автоматическую проверку элементов объекта информационных технологий на наличие ВП, выявление вредоносного воздействия и обезвреживание обнаруженных ВП.

Проведение испытаний ПСЗВВП и антивирусных программных средств на соответствие требованиям СТБ 34.101.8-2006 проводится с использованием коллекции тестовых вредоносных файлов.

Из сложившейся практики можно выделить следующие требования к тестовой коллекции:

а) размер тестовой коллекции должен быть равен суточному количеству ВП, детектируемых производителем антивирусного средства;

б) тестовая коллекция должна включать все известные типы угроз для операционных систем на которых проводятся испытания;

в) часть тестовых файлов подвергается модификации для испытаний антивирусного средства на «неизвестных» образцах.

За прошедшее с разработки стандарта время существенно увеличилось количество угроз безопасности объектам информационных технологий, что обусловило развитие СЗИ в данной области.

Перечисленные в текущей версии стандарта СЗИ позволяют обнаружить ВП, исполняемые в оперативной памяти либо хранящиеся на накопителе на жестких магнитных дисках, и предотвратить запуск ВП.

Исходя из жизненного цикла процесса заражения объектов информационных технологий появились дополнительно СЗИ способны дополнительно обнаруживать, идентифицировать и обезвреживать ПСЗВВП и АПС распространяемые по почте, и передаваемые по сети.

Данные виды ПСЗВВП и АПС часто интегрируются в программно-аппаратные комплексные решения, обеспечивающие многоуровневую защиту различных категорий компьютерных сетей.

С учетом особенностей новых видов СЗИ в проекте изменений к стандарту предлагается выделить дополнительные типы ПСЗВВП и АПС:

ПСЗВВП и АПС **четвертого типа** в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку пакетов сетевого трафика и обезвреживание обнаруженных ВП;

Требования к ПСЗВВП и АПС четвертого типа

Режим работы «Обработка объекта ИТ в реальном масштабе времени» должен обеспечить постоянную автоматическую обработку элементов объекта ИТ в течение работы объекта ИТ.

Подсистема контроля изменений

Требования к контролю изменений элементов объекта ОИТ не предъявляются.

Подсистема обнаружения должна обеспечивать:

а) обнаружение ВП, информация о которых известна;

б) обнаружение пассивных ВП;

в) идентификацию пассивных ВП, информация о которых известна.

Подсистема обезвреживания должна обеспечивать обезвреживание пассивных идентифицированных ВП.

Подсистема гарантированности свойств должна обеспечивать:

а) контроль целостности и актуальности баз, содержащих набор признаков известных ВП;

б) процедуру обновления набора признаков известных ВП;

в) процедуру обновления модулей обнаружения и обезвреживания ВП;

г) наличие эксплуатационной документации.

Подсистема регистрации должна обеспечивать:

а) регистрацию событий в журнале аудита по следующим параметрам:

1) дата/время;

2) объект ИТ/элемент объекта ИТ;

3) результаты обработки;

б) выдачу предупреждений об обнаружении ВП;

в) генерацию отчетов.

Допускается обеспечивать выдачу предупреждений об обезвреживании ВП.

ПСЗВВП и АПС **пятого типа** в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных ВП;

Режим работы «Обработка объекта ИТ в реальном масштабе времени» должен обеспечить постоянную автоматическую обработку элементов объекта ИТ в течение работы объекта ИТ.

Допускается дополнительно обеспечивать:

а) режим работы «Обработка объекта ИТ по запросу пользователя»;

б) режим работы «Обработка элементов объекта ИТ по заданному расписанию».

Подсистема контроля изменений

Требования к контролю изменений элементов объекта ОИТ не предъявляются.

Требования к подсистеме обнаружения

Подсистема обнаружения должна обеспечивать:

а) обнаружение ВП, информация о которых известна;

б) обнаружение пассивных ВП;

в) идентификацию ВП, информация о которых известна.

Рекомендуется обеспечивать обнаружение ВП, информация о которых отсутствует.

Требования к подсистеме обезвреживания

Подсистема обезвреживания должна обеспечивать обезвреживание пассивных идентифицированных ВП.

Рекомендуется обеспечивать обезвреживание вредоносных программ, информация о которых отсутствует.

Подсистема гарантированности свойств должна обеспечивать:

а) контроль целостности и актуальности баз, содержащих набор признаков известных ВП;

б) процедуру обновления набора признаков известных ВП;

в) процедуру обновления модулей обнаружения и обезвреживания ВП;

г) наличие эксплуатационной документации.

Подсистема регистрации должна обеспечивать:

а) регистрацию событий в журнале аудита по следующим параметрам:

1) дата/время;

2) объект ИТ/элемент объекта ИТ;

3) результаты обработки;

б) выдачу предупреждений об обнаружении ВП;

в) генерацию отчетов.

Допускается обеспечивать выдачу предупреждений об обезвреживании ВП.

Программные средства защиты от воздействия вредоносных программ и антивирусных программных средств **шестого типа** в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку эле-

ментов объекта ИТ на наличие ВП, выявление вредоносного воздействия и обезвреживание обнаруженных ВП;

Требования к ПСЗВВП и АПС шестого типа

Режим работы «Обработка объекта ИТ в реальном масштабе времени» должен обеспечить постоянную автоматическую обработку элементов объекта ИТ в течение работы объекта ИТ.

Подсистема контроля изменений

Допускается контроль изменений элементов объекта ОИТ.

Подсистема обнаружения должна обеспечивать:

а) обнаружение ВП, информация о которых известна;

б) обнаружение ВП, информация о которых отсутствует;

в) обнаружение пассивных ВП;

г) обнаружение активных ВП.

Подсистема обезвреживания должна обеспечивать:

а) обезвреживание активных идентифицированных ВП;

б) обезвреживание пассивных идентифицированных ВП;

в) обезвреживание ВП, информация о которых отсутствует.

Подсистема гарантированности свойств

Подсистема гарантированности свойств должна обеспечивать:

а) контроль целостности ПСЗВВП и АПС;

1) самоконтроль целостности модулей ПСЗВВП и АПС;

2) выдачу предупреждений при нарушении целостности;

б) наличие эксплуатационной документации.

Рекомендуется дополнительно обеспечить:

а) обновление набора признаков известных ВП;

б) обновление модулей обнаружения и обезвреживания ВП;

в) восстановление модулей ПСЗВВП и АПС при их повреждении.

Подсистема регистрации должна обеспечивать:

а) регистрацию событий в журнале аудита по следующим параметрам:

1) дата/время;

2) объект ИТ/элемент объекта ИТ;

3) результаты обработки;

б) выдачу предупреждений об обнаружении ВП;

в) генерацию отчетов.

Допускается обеспечивать выдачу предупреждений об обезвреживании ВП.

Программные средства защиты от воздействия вредоносных программ и антивирусных программных средств **седьмого типа** в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку файлов данных, передаваемых по сети, и обезвреживание обнаруженных ВП;

Требования к ПСЗВВП и АПС седьмого типа

Режим работы «Обработка объекта ИТ в реальном масштабе времени» должен обеспечить постоянную автоматическую обработку элементов объекта ИТ в течение работы объекта ИТ.

Подсистема контроля изменений

Требования к контролю изменений элементов объекта ОИТ не предъявляются.

Требования к подсистеме обнаружения

Подсистема обнаружения должна обеспечивать:

а) обнаружение ВП, информация о которых известна;

б) обнаружение пассивных ВП;

в) идентификацию ВП, информация о которых известна.

Рекомендуется обеспечивать обнаружение ВП, информация о которых отсутствует.

Требования к подсистеме обезвреживания

Подсистема обезвреживания должна обеспечивать обезвреживание пассивных идентифицированных ВП.

Рекомендуется обеспечивать обезвреживание ВП, информация о которых отсутствует.

Подсистема гарантированности свойств должна обеспечивать:

а) контроль целостности и актуальности баз, содержащих набор признаков известных ВП;

б) процедуру обновления набора признаков известных ВП;

в) процедуру обновления модулей обнаружения и обезвреживания ВП;

г) наличие эксплуатационной документации.

Подсистема регистрации должна обеспечивать:

а) регистрацию событий в журнале аудита по следующим параметрам:

1) дата/время;

2) объект ИТ/элемент объекта ИТ;

3) результаты обработки;

б) выдачу предупреждений об обнаружении ВП;

в) генерацию отчетов.

Допускается обеспечивать выдачу предупреждений об обезвреживании ВП.

ПСЗВВП и АПС **восьмого типа** после запуска по запросу пользователя должны обеспечивать проверку элементов объекта ИТ на наличие ВП и обезвреживание обнаруженных пассивных и активных ВП.

Требования к ПСЗВВП и АПС восьмого типа

Режим работы «Обработка объекта ИТ по запросу пользователя» должен обеспечивать однократную обработку элементов объекта ИТ.

Допускается обеспечивать периодическую автоматическую обработку элементов объекта ИТ согласно заданному расписанию

Подсистема контроля изменений

Требования к контролю изменений элементов объекта ОИТ не предъявляются.

Требования к подсистеме обнаружения

Подсистема обнаружения должна обеспечивать:

а) обнаружение ВП, информация о которых известна;

б) обнаружение активных ВП;

в) идентификацию активных ВП, информация о которых известна.

Рекомендуется обеспечивать обнаружение ВП, информация о которых отсутствует.

Требования к подсистеме обезвреживания

Подсистема обезвреживания должна обеспечивать:

а) обезвреживание активных идентифицированных ВП.

Рекомендуется обеспечивать обезвреживание ВП, информация о которых отсутствует.

Подсистема гарантированности свойств должна обеспечивать:

а) контроль целостности ПСЗВВП и АПС;

1) самоконтроль целостности модулей ПСЗВВП и АПС;

2) выдачу предупреждений при нарушении целостности;

б) процедуру обновления набора признаков известных ВП;

в) процедуру обновления модулей обнаружения и обезвреживания ВП;

г) наличие эксплуатационной документации.

Подсистема регистрации должна обеспечивать:

а) регистрацию событий в журнале аудита по следующим параметрам:

1) дата/время;

2) объект ИТ/элемент объекта ИТ;

3) результаты обработки;

б) выдачу предупреждений об обнаружении ВП;

в) генерацию отчетов.

Допускается обеспечивать выдачу предупреждений об обезвреживании ВП.».

Уточненная классификация позволит установить детальные требования для каждого типа ПСЗВВП и АПС с учетом их особенностей, что улучшит качество СЗИ допускаемых к распространению на рынке Республики Беларусь.

ПРИНЦИПЫ КЛАССИФИКАЦИИ И КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПО УРОВНЮ РИСКА

А.В. МИСЮК, В.К. ФИСЕНКО, М.П. ТУР

Белорусский государственный университет
Объединенный институт проблем информатики НАН Беларуси

Актуальность классификации по уровню риска

Современная информационная система (ИС) – это, прежде всего, совокупность модулей, собранных в соответствии с потребностями заказчика и формируются в соответствии с иерархией системой управления владельца системы или предприятия. Основные модули ИС формируются в соответствии с иерархией системы управления предприятием.

Под классификацией ИС по уровню риска понимаем систему соподчиненных понятий областей знаний по рискам информационной безопасности или деятельности человека, используемую как средство для установления связей между этими понятиями.

Таким образом, классификация ИС по уровню рисков означает систематизацию множества ИС на основании каких-то принципов, позволяющих объединить подмножества ИС в более общие классы.

Классифицировать современные ИС достаточно сложно. Это в первую очередь связано с тем, что системы обладают модульной конструкцией и предприятие имеет возможность закупать только необходимые ему компоненты. При этом одна фирма - поставщик, как правило, выпускает модули для различных областей. Однако, в настоящее время есть достаточно вариантов классификации ИС, среди которых можно выделить классификацию ИС по разным признакам риска, в том числе по степени автоматизации (ручные, автоматизированные (по сфере применения, по характеру обработки данных), автоматические) (рис. 1), а также по уровню управления, по типу данных.

Особо следует выделить классификацию ИС по требованиям защиты информации [1]. Установлено четыре класса защищенности ИС, каждый класс которых определяется уровнем значимости информации, обрабатываемой в информационной сис-