

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ  
Федеральное государственное бюджетное  
образовательное учреждение  
высшего профессионального образования  
**«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

---

**С. Л. ЗЕФИРОВ, А. Ю. ЩЕРБАКОВА**

# **УПРАВЛЕНИЕ ИНЦИДЕНТАМИ КИБЕРБЕЗОПАСНОСТИ**

***УЧЕБНОЕ ПОСОБИЕ***

**ПЕНЗА 2012**

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ  
Федеральное государственное бюджетное  
образовательное учреждение  
высшего профессионального образования  
«Пензенский государственный университет» (ПГУ)

---

С. Л. Зефилов, А. Ю. Щербакова

# Управление инцидентами кибербезопасности

*Учебное пособие*

Пенза  
Издательство ПГУ  
2012

УДК 004.056

З-47

**Рецензенты:**

кандидат технических наук, доцент,  
член-корреспондент Академии криптографии РФ,  
научный директор НПФ «Кристалл»

*В. В. Андрианов;*

председатель НТС филиала «Аргус»  
ОАО «Пензенский научно-исследовательский  
электротехнический институт»

*В. В. Коляда*

**Зефилов, С. Л.**

З-47      Управление инцидентами кибербезопасности : учеб. пособие / С. Л. Зефилов, А. Ю. Щербакова. – Пенза : Изд-во ПГУ, 2012. – 104 с.

ISBN 978-5-94170-559-7

Рассматриваются процессы и процедуры управления инцидентами информационной безопасности информационно-телекоммуникационной системы организации и управления инцидентами кибербезопасности: неавторизованный доступ, отказ в обслуживании, внедрение вредоносного кода, сбор информации. Учебное пособие разработано на основе источников, отражающих лучшие мировые и отечественные практики.

Подготовлено на кафедре «Информационная безопасность систем и технологий» и предназначено для студентов специальностей 090302 «Информационная безопасность телекоммуникационных систем» и 090303 «Информационная безопасность автоматизированных систем», изучающих вопросы управления инцидентами кибербезопасности в дисциплинах «Управление информационной безопасностью телекоммуникационных систем», «Менеджмент инцидентов информационной безопасности защищенных телекоммуникационных систем», «Управление информационной безопасностью», «Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления».

**УДК 004.056**

**ISBN 978-5-94170-559-7**

© Пензенский государственный  
университет, 2012

## СОДЕРЖАНИЕ

Введение.....	6
1. Система управления инцидентами кибербезопасности .....	8
1.1. Инциденты кибербезопасности. Процессы управления инцидентами.....	8
1.2. Планирование системы управления инцидентами информационной безопасности .....	10
1.2.1. Формирование политики управления инцидентами информационной безопасности .....	10
1.2.2. Формирование процедур управления инцидентами информационной безопасности .....	11
1.2.3. Создание группы реагирования на инциденты информационной безопасности .....	12
1.2.4. Подготовка к обработке инцидентов.....	13
1.2.5. Формирование последовательности действий при обработке инцидентов .....	13
1.2.6. Классификация инцидентов по значимости .....	16
1.2.7. Обеспечение осведомленности и обучение управлению инцидентами .....	17
1.3. Использование системы управления инцидентами информационной безопасности .....	18
1.3.1. Последовательность действий при обработке инцидента.....	18
1.3.2. Обнаружение и анализ инцидента.....	19
1.3.3. Реагирование на инциденты.....	23
1.4. Анализ обработки инцидентов.....	26
1.4.1. Изучение полученного опыта .....	26
1.4.2. Определение улучшения безопасности.....	27
1.4.3. Определение улучшения системы управления инцидентами.....	27
1.5. Улучшение системы управления инцидентами .....	28
1.5.1. Улучшение оценки рисков и управления информационной безопасностью .....	28
1.5.2. Улучшение безопасности .....	28
1.5.3. Улучшение системы управления инцидентами .....	28
Контрольные вопросы.....	28
2. Управление инцидентами неавторизованного доступа.....	30
2.1. Определение инцидента неавторизованного доступа. Цели инцидента неавторизованного доступа .....	30
2.2. Планирование системы управления инцидентами неавторизованного доступа .....	30
2.2.1. Подготовка к обработке инцидента.....	30
2.2.2. Выбор защитных мер .....	34

2.2.3. Формирование последовательности действий при обработке инцидентов неавторизованного доступа .....	36
2.2.4. Формирование порядка обработки инцидента неавторизованного доступа .....	37
2.3. Использование системы управления инцидентами неавторизованного доступа .....	38
2.3.1. Обнаружение и анализ инцидента неавторизованного доступа .....	38
2.3.2. Сдерживание инцидента неавторизованного доступа .....	43
2.3.3. Устранение инцидента неавторизованного доступа и восстановление после него .....	45
2.3.4. Сбор и обработка свидетельств инцидента неавторизованного доступа .....	46
Контрольные вопросы .....	46
3. Управление инцидентами отказа в обслуживании .....	47
3.1. Определение инцидента отказа в обслуживании. Примеры инцидентов отказа в обслуживании .....	47
3.2. Планирование системы управления инцидентами отказа в обслуживании .....	51
3.2.1. Подготовка к обработке инцидента .....	51
3.2.2. Выбор защитных мер .....	54
3.2.3. Формирование последовательности действий при обработке инцидентов отказа в обслуживании .....	55
3.2.4. Формирование порядка обработки инцидента отказа в обслуживании .....	57
3.3. Использование системы управления инцидентами отказа в обслуживании .....	57
3.3.1. Обнаружение и анализ инцидента отказа в обслуживании .....	57
3.3.2. Сдерживание, устранение инцидента отказа в обслуживании и восстановление после него .....	61
3.3.3. Сбор и обработка свидетельств инцидента отказа в обслуживании .....	62
Контрольные вопросы .....	62
4. Управление инцидентами внедрения вредоносного кода .....	63
4.1. Определение инцидента внедрения вредоносного кода. Примеры атак, связанных с внедрением вредоносного кода .....	63
4.2. Планирование системы управления инцидентами внедрения вредоносного кода .....	66
4.2.1. Подготовка к обработке инцидента .....	66
4.2.2. Выбор защитных мер .....	71
4.2.3. Формирование последовательности действий при обработке инцидентов внедрения вредоносного кода .....	72

4.2.4. Формирование порядка обработки инцидента внедрения вредоносного кода .....	74
4.3. Использование системы управления инцидентами внедрения вредоносного кода .....	75
4.3.1. Обнаружение и анализ инцидента внедрения вредоносного кода .....	75
4.3.2. Сдерживание и устранение инцидента внедрения вредоносного кода .....	81
4.3.3. Восстановление после инцидента внедрения вредоносного кода .....	84
4.3.4. Сбор и обработка свидетельств инцидента внедрения вредоносного кода .....	85
Контрольные вопросы .....	85
5. Управление инцидентами сбора информации .....	86
5.1. Определение инцидента сбора информации. Цели инцидента сбора информации .....	86
5.2. Планирование системы управления инцидентами сбора информации ...	86
5.2.1. Подготовка к обработке инцидента .....	86
5.2.2. Выбор защитных мер .....	89
5.2.3. Формирование последовательности действий при обработке инцидентов сбора информации .....	91
5.2.4. Формирование порядка обработки инцидента сбора информации ...	93
5.3. Использование системы управления инцидентами сбора информации ...	93
5.3.1. Обнаружение и анализ инцидента сбора информации .....	93
5.3.2. Сдерживание инцидента сбора информации .....	96
5.3.3. Устранение инцидента и восстановление после инцидента сбора информации .....	97
5.3.4. Сбор и обработка свидетельств инцидента сбора информации .....	97
Контрольные вопросы .....	97
Заключение .....	99
Библиографический список .....	100
Приложение. Сценарии инцидента .....	101

## Введение

Государственные и межгосударственные информационно-телекоммуникационные системы, сети общего пользования, трансграничные каналы передачи информации, в которых создается, перемещается и потребляется информация, образуют в совокупности мировое информационное пространство (киберпространство). Киберпространство для многих стран становится неотъемлемой частью управления экономикой и национальной безопасностью, для людей – средством общения, источником знаний. Киберпространство все больше внедряется в сферы деятельности человека, общества. С одной стороны, появляются новые возможности для деятельности человека, общества. С другой стороны, эта положительная тенденция сопровождается ростом преступности в глобальном информационном пространстве: кража активов, вывод из строя и нарушение функционирования систем, негативное информационное воздействие и т.д.

В России проблема преступности в киберпространстве (киберпреступности) носит актуальный характер, так как стремительное развитие информатизации в России несет в себе потенциальную возможность использования информационных и телекоммуникационных технологий в корыстных и других интересах, что в известной мере ставит под угрозу национальную и экономическую безопасность государства.

Проблемы борьбы с киберпреступностью должны решаться в правовой и технической области. Технические проблемы, возникающие в результате злоумышленной активности в глобальном информационном пространстве, – это сфера деятельности специалистов по информационной безопасности. В связи с возрастающим влиянием киберпространства на жизнедеятельность общества повышается значимость безопасности в киберпространстве (кибербезопасности) в областях обеспечения информационной безопасности.

Рекомендация МСЭ-Т X.1205 Overview of Cybersecurity определяет кибербезопасность как набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональную подготовку, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы электросвязи и всю со-