МОДЕЛЬ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КОРПОРАТИВНЫХ ОБРАЗОВАТЕЛЬНЫХ СЕТЕЙ

А.В. Усков
Государственный научно-исследовательский институт информационных технологий и телекоммуникаций «Информика», Москва
Тел.: (495) 629-45-34, e-mail: uskov@insightbb.com

Безопасность корпоративных образовательных сетей (КОС) остается актуальной проблемой для подавляющего большинства малых, средних и больших образовательных и тренинг организаций.

Анализ 246 докладов университетов США об успешных атаках вредоносных кодов или неправомерных нарушениях ИБ КОС [1] показывает, что 38% процентов успешных АВК были направлены на взлом серверов КОС, в 32% случаев – конфиденциальная информация была утеряна вследствие НПД (кража ноутбуков, дисков), в 21% случаев – успешными были АВК на веб-сервисы, ППО КОС и др.

Согласно докладу компании Computing Market Intelligence [2] на основе опроса более 60 ведущих корпораций США, среднестатистические финансовые потери в год от одного компьютера, использующего операционную систему Windows и допустившего проникновение вредоносных кодов разных типов, могут составлять от 281 до 340 долларов США. Принимая во внимание, что в образовательной организации могут обучаться тысячи и десятки тысяч студентов и работать несколько тысяч преподавателей, аспирантов и административных работников, финансовые потери от нарушения ИБ КОС могут исчисляться миллионами долларов США в год. Ярким свидетельством такого положения являются результаты опроса руководителей 592 университетов и колледжей США, проведенного в июне 2007 года ассоциацией EDUCAUSE [3]; они убедительно показывают, что вопросы ИБ КОС и ее объектов в 2006-2007 годах являлись вопросами первостепенной важности для администрации университетов США и останутся приоритетными вопросами на ближайшую обозримую перспективу. Дополнительно, в соответствии с обобщенными данными по вопросам безопасности КОС в 540 университетах и колледжах США за 2006-2007 годы [4], безопасность компьютерных сетей и данных является наиболее приоритетным вопросом в области информационных и коммуникационных технологий примерно 30% опрошенных организаций. Примерно в 67% опрошенных организаций бюджет на безопасность КОС достигает 10% от общего бюджета организации.

В связи с этими и многочисленными другими публикациями можно с уверенностью утверждать, что проблема надежной защиты информационных потоков и образовательных ресурсов КОС является одной из наиболее актуальных и значимых задач для современных образовательных организаций.

Одной из наиболее важных моделей информационной безопасности (ИБ) КОС является модель управления ИБ КОС, которая представляет собой структурированное описание организации единой интегрированной системы защиты информации в организации без рассмотрения конкретных деталей модели [5-8].

Разработанная интегрированная модель управления ИБ КОС определяет:

- уровни управления ИБ КОС;
- перечень превентивных и детективных мероприятий по различным видам безопасности КОС;
- информацию о вовлеченности разных групп администраторов и пользователей КОС в конкретное мероприятие ИБ.

Модель является инвариантной к конкретной ее реализации в той или иной образовательной организации. Более того, модель может быть легко адаптирована к специфике образовательной организации.

Уровни разработанной модели управления ИБ КОС включают:

- административный (высший уровень);
- сетевой (т.е. уровень распределенной компьютерной сети);
- информационный (т.е. уровень данных и информации в КОС);
- технический (т.е. уровень пользовательских компьютеров – офисных, домашних, переносных, с удаленным доступом, в учебных лабораториях и исследовательских центрах);
- физический (т.е. физическую охрану серверов данных, информационных и компьютерных центров и лабораторий, центров управления КОС и т.п.).

Каждый из указанных уровней управления ИБ КОС, в свою очередь, включает в себя как превентивные мероприятия, т.е. до обнаружения компьютерных атак и воздействия вредоносных кодов (АВК) мероприятия, так и детективные мероприятия, т.е. после обнаружения АВК или результатов их воздействия на КОС.

Участниками системы КОС являются следующие группы пользователей с существенно различными приоритетами доступа как в КОС в целом, так и к ее субъектам:

- ВР – высшее руководство образовательной организации, т.е. ректор, проректоры;
- РП – руководители крупных подразделений организации, т.е. деканы факультетов, директора центров, филиалов и представительств, начальники служб и подразделений;
- РБ – руководители служб всех типов безопасности организации;

- СА – разработчики КОС, провайдеры отдельных компонентов КОС и ее системные администраторы;
- ПР – преподаватели и разработчики образовательного контента;
- СС – студенты, аспиранты и сторонние пользователи КОС.

Основные компоненты разработанной модели управления ИБ КОС приведены в таблице 1.

Таблица 1. Модель управления информационной безопасностью КОС

Уровни управления и отдельные мероприятия по обеспечению информационной безопасности КОС		Вовлеченность участников КОС в мероприятие ИБ					
		ВР	РП	РБ	СА	ПР	СС
1. Административный уровень							
Превентивные средства		ВР	РП	РБ	СА	ПР	СС
1	Выработка стратегии и политик ИБ, утверждение стандартов, технологий и мероприятий ИБ КОС	X	X	X			
2	Выработка правил пользования объектов КОС	X	X	X	X		
3	Оценка возможных рисков и угроз для ИБ КОС	X	X	X	X		
4	Обучение (тренинг) по использованию средств ИБ КОС	X	X	X	X	X	X
Детективные средства		1	2	3	4	5	6
1	Немедленное реагирование на обнаруженные АВК, отражение АВК		X	X	X	X	X
2	Восстановление нормальной работоспособности КОС в целом и ее объектов в случае успешной АВК		X	X	X	X	X
3	Анализ причин успешной АВК; разработка новых или модификация существующих политик, технологий, средств, процедур и мероприятий ИБ	X	X	X	X	X	X
4	Аудит ИБ КОС на предмет отражения в будущем обнаруженной успешной АВК		X	X	X		
2. Сетевой уровень							
Превентивные средства		ВР	РП	РБ	СА	ПР	СС
1	Контроль доступа к объектам КОС			X	X		
2	Использование внешних и внутренних МЭ			X	X		
3	Создание и активное использование сетей VPN в КОС			X	X		
4	Шифрование информации и данных в сети			X	X		
5	Сканирование КОС на предмет уязвимостей в ИБ			X	X		
6	Мониторинг регистраций пользователей (логов) в КОС			X	X		
7	Мониторинг и анализ трафика в КОС			X	X		
8	Методика создания паролей (логинов) для входа в КОС и частоты смены паролей			X	X		
Детективные средства		ВР	РП	РБ	СА	ПР	СС
1	Немедленное оповещение субъектов КОС о потенциальных или обнаруженных АВК или НСД			X	X		
2	Обнаружение и исправление последствий АВК и несанкционированного доступа (НСД)			X	X		
3	Анализ регистраций (логов) в КОС			X	X		
3. Информационный уровень							
Превентивные средства		ВР	РП	РБ	СА	ПР	СС
1	Авторизация доступа в информационным ресурсам		X	X	X		
2	Управление модификацией и изменением данных и информации в КОС по их типу, стандартам, протоколам и назначению; обеспечение полной совместимости новых и старых данных			X	X		
3	Шифрование информации и данных, хранящихся в КОС на основе криптографических алгоритмов, стандартов и протоколов ИБ			X	X	X	X
4	Управление системой приоритетов доступа к информационным ресурсам КОС			X	X	X	X
5	Мониторинг источников изменения информации и генераторов данных в КОС				X	X	X
6	Регулярное создание резервных копий основных информационных ресурсов КОС			X	X	X	X

7	Распределение обязанностей по хранению данных и информации в КОС, мониторингу их изменений			X	X	X	X
Детективные средства		ВР	РП	РБ	СА	ПР	СС
1	Анализ регистраций (логов) в КОС			X	X		
2	Обнаружение несанкционированных изменений в данных и информационных ресурсах КОС и их исправление			X	X		
4. Технический уровень (уровень пользовательских компьютеров - ПК)							
Превентивные средства		ВР	РП	РБ	СА	ПР	СС
1	Конфигурирование ПК в соответствии с требованиями системы ИБ КОС и регистрация ПК в КОС			X	X	X	X
2	Конфигурирование средств ИБ и сетей VPN на ПК			X	X	X	X
3	Контроль доступа в КОС с зарегистрированных ПК			X	X		
4	Сканирование ПК на предмет АВК и уязвимостей ИБ			X	X	X	X
5	Шифрование данных на ПК					X	X
6	Мониторинг источников информации на ПК					X	X
7	Немедленная инсталляция всех вновь появляющихся от компаний-производителей программных усовершенствований (updates) или «заплаток» (patches) на системное (операционная система) и прикладное (пакеты программ) программное обеспечения ПК				X	X	X
8	Регулярное обучение (тренинг) по ИБ КОС			X	X	X	X
Детективные средства		ВР	РП	РБ	СА	ПР	СС
1	Оповещение пользователей об обнаружении АВК или НСД к КОС с ПК				X		
2	Обнаружение и исправление результатов АВК и НСД на ПК				X	X	X
3	Обеспечение целостности и конфиденциальности данных (файлов) пользователей на ПК				X	X	X
5. Физический уровень							
Превентивные средства		ВР	РП	РБ	СА	ПР	СС
1	Правила и часы использования компьютерных лабораторий, центров, офисов, серверных центров и т.п.	X	X	X	X	X	X
2	Закрываемые на ключ (электронный или физический) и находящиеся под охраной помещения организации	X	X	X	X	X	
3	Мониторинг основных помещений с расположенными в них центральными серверами КОС, дистанционное видео наблюдение и запись на видеокамеры всех входящих, выходящих и работающих сотрудников КОС, и времени их работы		X	X			
4	Мониторинг помещений организации на предмет возможных краж оборудования КОС и ПК		X	X			
5	Патрулирование компьютерных центров и лабораторий организации (особенно, в ночное время)			X			
6	Физическая защита компьютеров и периферийных устройств с использованием замков, датчиков и т.п.			X			
7	Физическая защита электрических кабелей, экранизация от электромагнитных наводок			X			
8	Противопожарные средства			X			
9	Климатический контроль помещений			X			
Детективные средства		ВР	РП	РБ	СА	ПР	СС
1	Средства оповещения о НСД в помещения организации		X	X			
2	Средства оповещения о НПД в отношении объектов КОС (например, кражах оборудования)		X	X			

Практические реализации модели управления ИБ КОС могут существенно отличаться друг от друга в зависимости от:

- масштаба образовательной организации и размеров ее КОС, т.е. от количества ее пользователей, обслуживающего технического персонала, подсетей КОС, используемых каналов связи с подразделениями и т.п.;

- структурной модели образовательной организации, например, а) отдельный университет или колледж, б) организация с центральным отделением (университетом) и многими географически распределенными ее подразделениями (кафедрами, филиалами, обучающими центрами и т.п.), в) ассоциация географически распределенных университетов или колледжей без центрального отделения (университета) и др.;
- объема финансирования мероприятий по обеспечению ИБ КОС;
- степени использования а) коммерческих продуктов третьих сторон, б) провайдеров Интернета, беспроводной сети, серверов вне пределов образовательной организации, в) аутсорсинга используемых программных приложений и образовательного контента КОС, технологий ИБ и т.п.

Литература

1. Conway W. Information Security Breaches: 2000-2007 // http://www.walterconway.com.
2. Computing Market Intelligence // http://www.computingmi.co.uk.
3. Camp J., et al. 2007 EDUCAUSE Current Issues Committee Report: Top 10 IT Issues // http://www.educause.edu.
4. The 2007 National Survey of Information Technology in U.S. Higher Education // http://www.campuscomputing.net/survey.
5. K. Green, The 2007 National Survey of Information Technology in US Higher Education, The Campus Computing Project.
6. Мельников В. П. и др. Информационная безопасность. // М.: Академия, 2005. – 333 с.
7. Сердюк В. Новое в защите от взлома корпоративных систем // М.: Техносфера, 2007. – 360 с.
8. Петренко С.А., Курбатов В.А. Политики информационной безопасности // М.: Компания АйТи, 2006. – 400 с.