УДК 004.056

Ермолова Т.С.

студентка

4 курс, факультета «Бизнеса и рекламы»

Орловский государственный университет экономики и торговли

Россия, г. Орёл

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ МЕСТО В ПОЛИТИКЕ БЕЗОПАСНОСТИ

Аннотация: В статье рассмотрен передовой опыт ряда крупных компаний, были описаны основные этапы разработки политики безопасности компании в IBM, Sun и Symantec. Также был изучен опыт компании Cisco. Рассмотрены основные показатели эффективности защиты информации. Также была проведена сравнительная характеристика наиболее популярных систем защиты информации.

Ключевые слова: защита информации, информационная безопасность, корпоративная сеть, методы защиты информации; политика безопасности, система защиты безопасности, эффективность защиты информации.

Ermolova T.S.

student

4 course, faculty of «Business and advertising»

The Orel State University of Economics and Trade

Russia, Orel

THE INFORMATION SECURITY SYSTEM AND THEIR PLACE IN THE SECURITY POLICY

Abstract: The article describes the best practices of a number of large companies, described the main stages of development of the company's security policy in IBM, Sun and Symantec. The experience of Cisco was also studied. The main indicators of effectiveness of information protection. Comparative

characteristics of the most popular information security systems were also carried out.

Keywords: information security, information security, corporate network, methods of information security; security policy, security protection system, the effectiveness of information security.

Информация сегодня – важный ресурс, потеря которого чревата неприятными последствиями. Потеря конфиденциальной информации компании может привести к финансовым потерям, так как полученной информацией могут воспользоваться конкуренты или злоумышленники. В целях предотвращения нежелательных ситуаций все современные компании и учреждения используют методы защиты информации [1].

Качество функционирования информационной системы во многом определяется уровнем защиты от внешних воздействий.

Мировая и российская статистика свидетельствует о тенденции роста масштабов компьютерного неправомерного использования, что может привести к значительным финансовым потерям хозяйствующих субъектов разного уровня. Так, число компьютерных преступлений в РФ выросло с 1997 года по2005 год, примерно в 150 раз [2].

Растущая потребность в надежной защите данных во время обработки в ненадежной среде создает беспрецедентные проблемы для компьютерной индустрии [3]. Нарушение эффективности автоматизированных систем, в том числе из-за нарушения установленного режима информационной безопасности, может привести к серьезным последствиям. Это особенно важно для систем контроля критических объектов-автоматизированных систем контроля [4]. Информационная безопасность представляет собой комплекс мер по обеспечению наиболее важных аспектов информационной безопасности. Система информационной безопасности – это набор кадровых ресурсов структурных подразделений, предназначенных для защиты информации, методов и средств защиты информации, а также объектов

защиты, организованных и функционирующих в соответствии с правилами и нормативными актами, принятыми в сфере информационной защиты [5]. Основным законом в области информации является Федеральный закон «Об информации, информационных технологиях и защите информации» общие понятия и принципы применимы ко всей информационной сфере, за исключением случаев, когда общие и особые нормы конкурируют (рисунок 1).

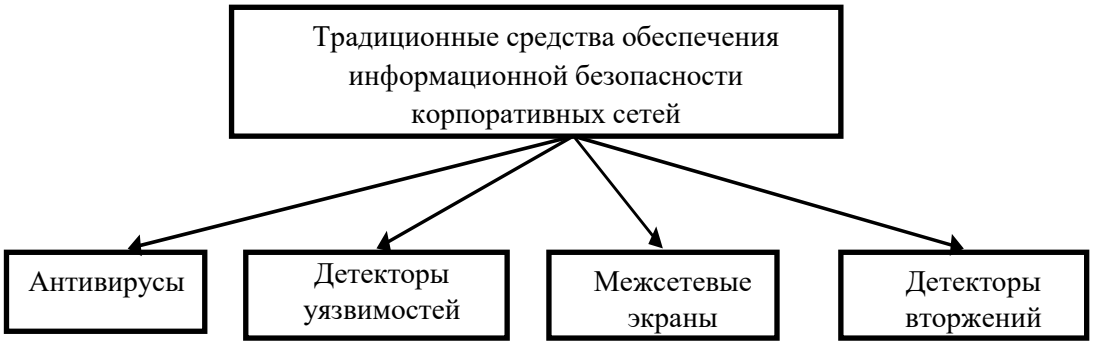

Рисунок 1 – Традиционные средства обеспечения информационной безопасности корпоративных сетей

Основными угрозами для информационной безопасности и нормального функционирования информационных систем являются:

– утечка конфиденциальной информации;

– компрометация информации;

– ошибочное использование информационных ресурсов.

Чтобы устранить и предотвратить информацию, представляющую угрозы различного характера, необходимо создать четкую систему управления инцидентом, которая основана на требованиях, учитывающих мнения всех владельцев участвующих бизнес-процессов.

Комплексная система резервного копирования информации должна отвечать следующим требованиям:

– оперативно реагировать на изменения определяющие методы и

средства защиты;

– иметь удобную и достаточную надежность, обеспечивающую безопасность при работе с информацией;

– иметь элементы идентификации пользователей;

– надежность контроля передаваемой, экономической информации;

– обеспечение провидения учета и расследования случаев нарушения безопасности;

– использование комплекса программно - технических средств и организационных мер по защите комплексной системы [6].

Проблема информационной безопасности остается по сей день важной. Развитие электронно-вычислительных машин, появление персональных компьютеров во второй половине XX века позволили значительно упростить множество сложных и трудоемких математических операций, используемых при анализе экономической информации. Однако степень защищенности информации значительно снизилась [8].

Специальные методы защиты информации для предотвращения ряда угроз:

– предварительное шифрование;

– криптографические методы;

– прозрачное шифрование.

При разработке или выборе системы безопасности следует учитывать особенности объекта и ряд стандартов. Следует отметить, что ряд зарубежных компаний рекомендуют использовать международный стандарт ISO 17799:2002.

По мнению IBM, разработка методических документов в области безопасности должна начинаться с создания политики информационной безопасности компании. Рекомендуется использовать международный стандарт ISO 17799: 2002 и политику безопасности компании, которая будет рассматриваться как часть процесса управления информационными рисками

[11].

Передовой опыт таких ведущих ИТ-компаний, как IBM, Sun, Symantec подтверждает необходимость пошаговой реализации решений в области информационной безопасности. В таблице 1 представлены этапы разработки политики безопасности компаний.

Таблица 1 – Этапы разработки политики безопасности компании в IBM, Sun и Symantec

Компания	Этапы разработки политики безопасности компании
IBM	- анализ бизнес-стратегии компании и связанные с этим требования по информационной безопасности; - анализ ИТ-стратегии, текущие проблемы информационной безопасности и требования по информационной безопасности, которые появятся в будущем; - создание политики безопасности, взаимно увязанной с бизнес- и IT-стратегиями.
Sun	- определение основных целей и задач развития бизнеса компании; - описание основных принципов безопасности; - классификация и категорирование информационных ресурсов; - анализ информационных потоков; - определение основных угроз и модели нарушителя; - определение сервисов безопасности; - создание шаблона политики безопасности; - определение области действия политики безопасности.
Symantec	- определение и оценка информационных активов; - определение угроз безопасности; - оценка информационных рисков; - определение ответственности; - создание комплексного документа; - реализация; - управление программой безопасности.

Принимая во внимание основные этапы развития политики безопасности компании IBM, Sun и Symantec можно сделать вывод, что основным принципом является основные цели развития и, следовательно, безопасность информации должна обеспечить динамическое развитие бизнеса и реализацию изложенных стратегических целей.

Положительный опыт Sun был основан на «нисходящем» подходе, то есть сначала политика безопасности, а затем в соответствующих условиях разрабатывается архитектура системы информационной безопасности компании.

Опыт компании Cisco также замечен. Для бесперебойной работы ИТ-систем, была разработана специальная матрица, где приведены основные типы пользователей и степень риска для каждой группы системной информации. Эта матрица дала возможность унифицировать ряд систем для обеспечения качества работы в сфере безопасности.

Для того, чтобы создать реалистичную политику безопасности предприятия (Sun Microsystems), необходимо, чтобы это были разумные цели и задачи развития бизнеса компании. Для этого необходимо понятие управления информационными рисками. В теории финансового управления Категория риска определяется следующим образом [10]:

$$R = H \times P, \qquad (1)$$

где H – денежная оценка ущерба в результате инцидента,

P – вероятность инцидента.

Высокий спрос на программные продукты для защиты информации от несанкционированного доступа и привел к быстрому развитию рынка для рода программных продуктов. TrueCrypt, Аура, Dallas Lock 8.0-K, SecretNet 7 стали самыми популярными.

Система защиты информации от несанкционированного доступа Аура используется для комплексной защиты информации в автоматизированных системах. Аура была разработана для защиты рабочих станций от несанкционированного доступа. Dallas Lock 8.0-K защищает конфиденциальную информацию, определяя права доступа пользователя к файловой системе и другим ресурсам. SecretNet 7 обеспечивает защиту персональных данных и государственной тайны [12; 13; 14].

Таблица 2 – Сравнительная характеристика систем защиты информации

Система защиты информации	Преимущества	Недостатки
TrueCrypt	Высокая скорость шифрования данных. Использовать несколько алгоритмов блочного симметричного шифрования данных на выбор. Возможность создания скрытых контейнеров внутри зашифрованных. Не сохраняет промежуточные данные на диск, а хранит в оперативной памяти (отсутствует доступ к ключам во временных файлах).	Ориентированность на Windows- системы. Нет возможности изменения контейнера. Нет встроенного генератора паролей. Есть вероятность полной потери данных при удалении файла-контейнера. Смонтированный том TrueCrypt виден и доступен для всех пользователей без исключения (избежать доступа можно при использовании разрешений NTFS).
Аура	Многоуровневый контроль целостности информационных объектов вычислительной системы. Регистрация действий пользователя и событий в системных журналах. Прозрачное кодирование носителей информации. Идентификация и аутентификация пользователей в доверенной среде. Поддержка ГОСТ Р 51241-2008, ГОСТ 34003-90 и ГОСТ 34.602-89.	Ориентированность на Windows – системы. Разграничение доступа к устройствам действует на уровне шины по классам устройств, не идентифицируя конкретное устройство. Метки на объекты файловой системы устанавливаются только на файловой системе NTFS.
Dallas Lock 8.0-K	Дискреционный и мандатный принципы контроля доступа к файловой системе. Поддержка замкнутой программной среды. Подсистема очистки остаточной информации. «Домен безопасности». Функция аварийного удаления Dallas Lock с помощью диска.	Ориентированность на Windows- системы. Нельзя работать с системой средствами командной строки для создания сценариев автоматизации некоторых процедур.
SecretNet	Автономный и сетевой режимы. Можно задать необходимый уровень управления в организациях различного размера. Наличие единого централизованного управления и мониторинга безопасности в режиме реального времени.	Ориентированность на Windows- системы.

Современные информационные системы безопасности позволяют решать ряд стратегически важных задач, но выбор должен быть учтен

главным фактором-стратегией компании, которая определяет окончательный выбор системы. Качество реализации политики в сфере информационной безопасности необходимо периодически анализировать и определять ее эффективность.

Использованные источники:

1. Ахметова Н. О. Основные методы защиты информации на предприятиях // Актуальные вопросы в научной работе и образовательной деятельности сборник научных трудов по материалам Международной научно-практической конференции: в 10 томах. 2015. С. 9–11.
2. Сагатбекова Д. Е., Амиров А. Ж., Сексенбаев К., Кожанов М. Г. Методы и модели оценки инфраструктуры системы защиты информации в корпоративных сетях в вузах РК // Научный альманах. 2015. № 10–3 (12). С. 221–224.
3. Бабенко Л. К., Буртыка Ф. Б., Макаревич О. Б., Трепачева А. В. Обобщенная модель системы криптографически защищенных вычислений // Известия ЮФУ. Технические науки. 2015. № 5 (166). С. 77–88.
4. Камаев В. А., Натров В. В. Анализ методов оценки качества функционирования и эффективности систем защиты информации на предприятиях электроэнергетики // Известия Волгоградского государственного технического университета. 2007. Т. 1. № 1 (27). С. 74–76.
5. Альшанская Т. В. Управление службой защиты информации на основе современных методов // Информационные системы и технологии: управление и безопасность. 2013. № 2. С. 81–86.
6. Гольтяпина И. Ю. Система информационного законодательства: вопросы теории // Проблемы права. 2014. № 3. С. 95–99.
7. Черней Г. А., Охрименко С. А., Ляху Ф. С. Безопасность автоматизированных информационных систем. Ruxanda, 1996. 186 с.
8. Суслов С. А., Завиваев Н. С., Генералов И. Г., Черемухин А. Д. Роль информационных технологий в повышении конкурентоспособности

региональных рынков // Дискуссия. 2015. № 8. С. 45–49.

9. Петренко С. А., Курбатов В. А. Лучшие практики создания нормативных документов по кибербезопасности в компании // Труды Института системного анализа Российской академии наук. 2006. Т. 27. С. 177–233.

10. Заболотский В. П., Юсупов Р. М. Применение метода индексов для оценивания эффективности защиты информации // Труды СПИИРАН. 2006. Т. 2. № 3. С. 70–83.

11. Бикмаева Е. В., Баженов Р. И. Об оптимальном выборе системы защиты информации от несанкционированного доступа // APRIORI. Серия: Естественные и технические науки. 2014. № 6. С. 5.

12. Средства защиты информации от несанкционированного доступа Dallas Lock. [Электронный ресурс]. URL:http://www.4systems.ru/catalog/category/ dnd/Confident (дата обращения: 19.08.2016).

13. Средства защиты информации от несанкционированного доступа Secret Net. [Электронный ресурс]. URL: http://www.4systems.ru/catalog/category/ dnd/SecretNet (дата обращения: 19.08.2016).

14. СЗИ от НСД Secret Net. [Электронный ресурс]. URL:http://www.securitycode.ru/products/secret_ net/ (дата обращения: 19.08.2016).