ПРОГРЕССИВНЫЕ, СПЕЦИАЛЬНЫЕ И НЕТРАДИЦИОННЫЕ ТЕХНОЛОГИИ

ЗАЩИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ ОТ ВНЕШНИХ ВОЗДЕЙСТВИЙ

Щербов И.Л., Джура Г.С., *(кафедра радиотехники и защиты информации, ИГЗД ДонНТУ, г. Донецк, ДНР)*

В современных условиях использование информационных технологий в процессах государственного управления, управления бизнесом, производственными процессами, удовлетворение потребностей граждан на обеспечение свободного доступа к информации способствует развитию информационных, телекоммуникационных и информационно-телекоммуникационных систем (ИТС).

Постановка задачи.

Развитие инфраструктуры ИТС позволяет сократить расстояния между взаимодействующими субъектами, уменьшить время на обмен информацией и, как следствие, позволяет ускорить процесс принятия управленческих решений.

Рассредоточенное расположение субъектов, связанных общими целями и задачами требует оптимального проектирования и эффективного управления информационной безопасностью в ИТС.

Для решения задачи по защите информации в ИТС ее следует рассматривать как сложную систему, включающую значительное количество взаимосвязанных информационных и телекоммуникационных систем. При решении данной задачи возникает ряд проблем, наиболее сложными из которых являются:

- координация действий между отдельными составляющими, которые принадлежат разным владельцам;
- влияние внешних и внутренних деструктивных факторов;
- ограниченные финансовые возможности.

В представленной работе на примере выбора программных и программно-аппаратных средств защиты информации с целью обеспечения безопасности ИТС организации от DoS/DDoS-атак предложен вариант принятия решения на организацию защиты исходя из критериев, установленных в техническом задании, а именно: достижение необходимого уровня защиты информации с ограниченным доступом при минимальных затратах и допустимом уровне ограничений видов информационной деятельности.

Пути решения задачи.

Причины возникновения DDoS-атак можно подразделить на следующие:

-Конкуренция;

-Мошенничество;

-Развлечение либо забава.

Наиболее распространенных сценариев DDoS-атак два: запросы от большого количества ботов напрямую к атакуемому ресурсу (сценарий 1 на рис. 1) или запросы от ботов, усиленные с использованием публично доступных серверов с уязвимым программным обеспечением (сценарий 2А на рис. 1). В первом случае злоумышленники превращают множество компьютеров в удаленно контролируемые «зомби» (боты), которые затем одновременно по команде хозяина ботнета отправляют на интернет-ресурс жертвы какие-либо запросы (осуществляют «распределенную атаку»). Иногда вместо ботнета используется завербованная хакерами группа пользователей, снабженная спе-

циальными программами для осуществления DDoS-атаки.

При втором сценарии, то есть при усиленной атаке, вместо ботов также могут быть использованы арендованные в дата-центре серверы (сценарий 2Б на рис. 1), а для усиления, как правило, применяются публичные серверы с уязвимым ПО. В данный момент распространены два варианта усиления - через серверы системы доменных имен (DNS) или серверы синхронизации времени (NTP). Усиление атаки производится за счет подмены обратных IP-адресов и отправки на сервер короткого запроса, который требует гораздо более объемного ответа. Полученный ответ отсылается на подменный IP-адрес, принадлежащий жертве. Сценарии проведения DDoS-атак изображены на рис. 1.

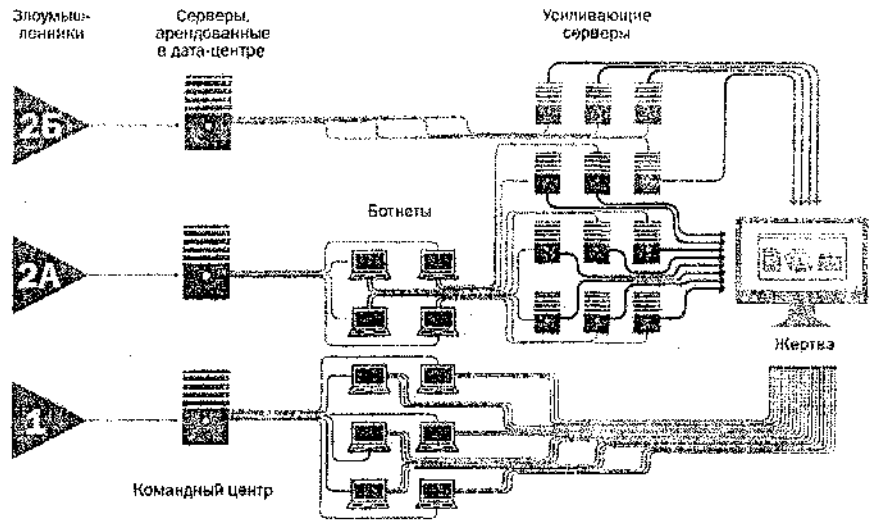

Рис. 1. Возможные сценарии DDoS-атак

В первом квартале 2015 года, как и в четвертом квартале 2014, наиболее популярным методом DDoS-атаки стал SYN-DDoS. Атаки типа TCP-DDoS уступили второе место HTTP.

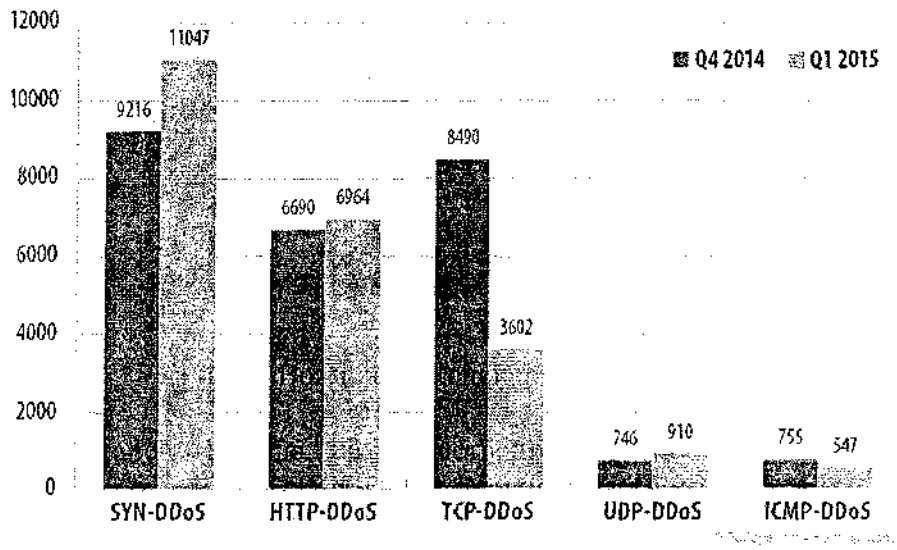

Рис. 2. Наиболее популярные типы DDoS - атак в 2014- 2015 годах

Количество охваченных стран, число и мощность DDoS-атак растет с каждым годом. Традиционно больше всего атак приходится на ресурсы из США и Китая, так как в этих странах дешевый хостинг и в них расположены многие ресурсы.

Защита от DDoS-атак предусматривает 2 направления: (защита от DDoS-атак, направленных за пределы сети, защита от внешних DDoS-атак).

В данной работе были рассмотрены следующие программно и программно-аппаратные средства защиты:

4. CDN-сервис «Cloud Flare»
5. Программно-аппаратный продукт «Kaspersky DDoS Prevention»
6. Программный продукт Cisco Security Agent 4.5
7. Программно-аппаратный продукт «Периметр»

Выбор программных и программно-аппаратных средств защиты - это динамичный, циклический процесс, который должен учитывать задачи, возникающие в соответствии с этапами жизненного цикла ИТС.

На рисунке 3 представлена исследуемая информационная система.

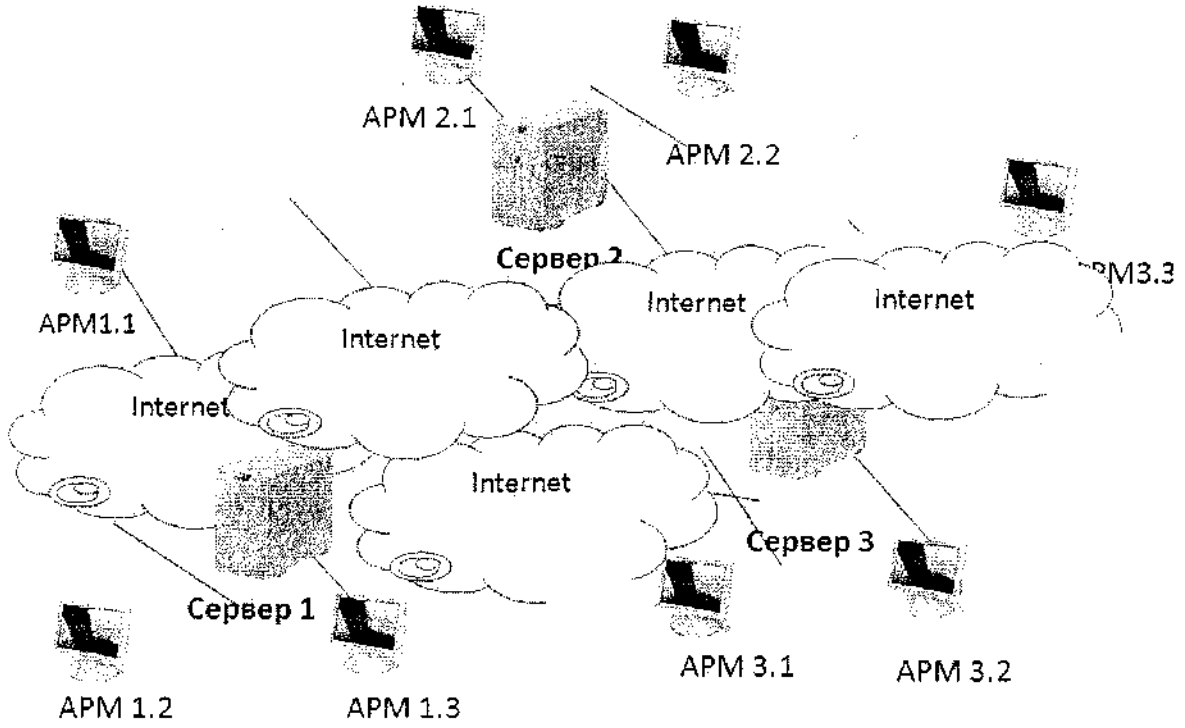

Рисунок 3 - Структура исследуемой ИТС

Угрозы для информационной безопасности ИТС, которые могут быть реализованы с использованием протоколов межсетевого взаимодействия и их влияние на свойства информации представлены в таблице 1.

Таблица 1. Угрозы для информационной безопасности ИТС

№ пп	Угрозы	Конфиденциальность	Целостность	Доступность	Наблюдаемость, управляемость	Весовой коэффициент
1	DDoS-атака	c_1	i_1	a_1	s_1	p_1
2	Сканирование сети	c_2	i_2	a_2	s_2	p_2
3	Автоматический подбор паролей	c_3	i_3	a_3	s_3	p_3

Определение уровня опасности угрозы необходимо проводить экспертным методом или эмпирическим путем, на основании опыта эксплуатации подобных систем, путем привлечения специалистов структурных подразделений в интересах которых будет эксплуатироваться ИТС.

Оценка должна состоять из величин ожидаемых убытков от потери информации каждой из свойств (конфиденциальности, целостности или доступности) или от потери управляемости ИТС в результате реализации угрозы. Для оценки угрозы рекомендуется вводить несколько дискретных ступеней (градаций).

Определения уровня опасности угрозы (threat) для свойств информации, циркулирующей в ИТС осуществляем по формуле:

$$T = \sum \frac{\{c_k + i_k + a_k + s_k\}}{4} \cdot p_k \quad T = \sum \frac{\{c_k + i_k + a_k\}}{3} \square p_j \,, \qquad (1)$$

Где, c_k - угрозы, влияющие на конфиденциальность информации, i_k - угрозы, влияющие на целостность, a_k - на доступность, s_k - угрозы, влияющие на наблюдательность информации, численно определяется по пяти бальной шкале, p_k - весовой коэффициент, определяет стоимость конкретного средства защиты относительно всех возможных средств защиты, которые могут быть применены при построении комплексной системы защиты информации.

Данные, приведенные в таблице были взяты на основании полученных экспертных оценок и анализа документации выбранных продуктов.

Вероятность отражения угрозы программными и программно-аппаратными средствами защиты приведена в таблице 2.

Таким образом используя предложенный алгоритм для анализа ожидаемой защищенности ИТС от возможных угроз для рассматриваемых средств защиты для каждой точки соприкосновения ИТС с телекоммуникационной сетью, мы определяем программные и программно-аппаратные средства защиты, которые отвечают определенным требованиям: достижение необходимого уровня защиты информации с ограниченным доступом при минимальных затратах и допустимого уровня ограничений видов информационной деятельности (ИД) и будут использованы при построении комплексной системы защиты информации.

Таблица 2. Вероятность отражения угрозы средствами защиты

п	Угрозы	CDN-сервис «CloudFlare»	«Kaspersky DDoS Prevention»	«Cisco Security Agent 4.5»	«Периметр»
	DDoS-атака	0,7	0,96	0,8	0,9
	Сканирование сети	0,59	0,97	0,89	0,51
	Автоматический подбор паролей	0,75	0,6	0,91	0,93

Исходя из функций, которые выполняют программные и программно-аппаратные средства защиты, а также из уровня опасности угрозы для свойств информации, обрабатываемой на отдельном сервере (АРМ), мы можем вычислить ожидаемую защищенность ИТС от возможных угроз конкретным средством защиты:

$$Q = \sum \frac{\{c_k + i_k + a_k + s_k\}}{4} \cdot p_k \cdot z_k, \quad (1)$$

где z_k - вероятный процент отражения k угрозы определенным средством защиты.

В следующей таблице представлены результаты, полученные в результате расчета эффективности использования для одного из средств защиты.

Таблица 3. Исходные данные для расчета эффективности использования CDN-сервиса «CloudFlare»

	c_k	i_k	a_k	s_k	p_k	z_k
Сервер 1	0	0	0,75	0,75	0,2	0,7
Сервер 2	0	0	0,5	0,5	0,2	0,7
Сервер 3	0	0	0,25	0,25	0,2	0,7
АРМ 1	0	0	0	0	0	0
АРМ 2	0	0	0	0	0	0

Таким образом используя предложенный алгоритм для анализа ожидаемой защищенности ИТС от возможных угроз для рассматриваемых средств защиты для каждой точки соприкосновения ИТС с телекоммуникационной сетью, мы определяем программные и программно-аппаратные средства защиты, которые отвечают определенным требованиям: достижение необходимого уровня защиты информации с ограниченным доступом при минимальных затратах и допустимого уровня ограничений видов информационной деятельности (ИД) и будут использованы при построении комплекс-

ной системы защиты информации.

Используя полученные экспертные оценки по определению уровня опасности угрозы для серверов и автоматизированных рабочих мест; имеющиеся статистические данные вероятности защиты рассмотренных программных и программно-аппаратных средств защиты от DDoS-атак, а также стоимость рассматриваемого средства защиты, получим относительную эффективность применения данного средства.

Таблица 4. Результаты анализа целесообразности применяемого средства защиты

№	Средства защиты	Результаты анализа
1	«CloudFlare»	0.105
2	«Kaspersky DDoS Prevention»	0.216
3	«Cisco Security Agent 4.5»	0.12
4	«Периметр»	0.203

Выводы

В ходе работы были проанализированы внешние угрозы для информационно-телекоммуникационной системы предприятия на примере DDos-атак. Рассмотрены основные причины их возникновения, классификация и статистика зафиксированных случаев проведения.

Рассмотрены методы и средства защиты ИТС предприятия от внешних воздействий.

Проведен анализ следующих программных и программно-аппаратных средств защиты: CDN-сервис Cloud Flare, программно-аппаратный продукт «Kaspersky DDoS Prevention», программный продукт «Cisco Security Agent 4.5» и программно-аппаратный продукт «Периметр». Рассмотрены достоинства и недостатки данных средств защиты.

Предложен алгоритм принятия решения по выбору наиболее эффективных средств защиты информационно-телекоммуникационной системы предприятия от внешних угроз и проведен математический расчет.

Список литературы: 1. Воропаева, В. Я., Управление информационной безопасностью информационно-телекоммуникационных систем на основе модели «plan-do-check-act»/ **2.** В. Я. Воропаева, И. Л. Щербов, Е. Д. Хаустова // Научные работы-Донецк: ДонНТУ. Серия: Вычислительная техника и автоматизация. Выпуск 25. - Донецк, ДонНТУ, 2013. С - 104-110. **3.** Аноприенко, А. Я. Особенности моделирования и оценки эффективности работы сетевой инфраструктуры/ **4.** А. Я. Аноприенко, С. Н. Джон, С. В. Рычка// Научные работы - Донецк: ДонНТУ, 2002. Серия: «Вычислительная техника и автоматизация». Выпуск 38 - С. 205 – 210. 5. ITU-T X.80 **5.** Security architecture for systems providing end-to-end communications. **6.** ISO/IEC 27005. Information technology - Security techniques - Information security risk management. **7.** Воропаева, В. Я. Адаптирование информационно-телекоммуникационных систем к внешним воздействиям /, В. Я. Воропаева, И.Л. Щербов// Научные работы Донецк: ДонНТУ. Серия: Вычислительная техника и автоматизация. Выпуск 23 (201). - Донецк, ДонНТУ, 2012. - С 83-88.