КОМПЛЕКСНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИИ И ЗА РУБЕЖОМ

Рубцов Артем Михайлович
студент 1 курса факультета информационных технологий,
Направление: Прикладная математика и информатика,
Московский политехнический университет

Тюменев Александр Владимирович
начальник управления комплексной безопасности,
Московский политехнический университет

Аннотация: *В статье проанализированы: системы информационной безопасности, виды угроз, методы и способы защиты информации от несанкционированного доступа, законы о защите информации, число атак на ПК, методы обеспечения информационной безопасности, особенности информационной безопасности в ВУЗах.*

Abstract: *The article analyzes the system of information security, types of threats and methods to protect information from unauthorized access, laws on the protection of information, the number of attacks on PC, methods of information security, especially information security in higher education.*

Ключевые слова: *Информационная безопасность, закон, управления информационными ресурсами системы высшего образования в РФ.*

Key words: *Information security, law, management of information resources of the higher education system in the Russian Federation.*

Введение. В современных условиях всеобщей информатизации и развития информационных технологий усиливаются угрозы национальной безопасности Российской Федерации в информационной сфере.

Концепцию национальной безопасности РФ применительно к информационной сфере развивает Доктрина информационной безопасности Российской Федерации. В Доктрине указывается, что обеспечение информационной безопасности РФ играет ключевую роль в обеспечении национальной безопасности РФ. При этом одним из приоритетных направлений государственной политики в области обеспечения информационной безопасности РФ является совершенствование подготовки кадров, развитие образования в области информационной безопасности. Особую роль в решении этих задач играют вузы. Российская высшая школа переживает период адаптации не только к объективным процессам информационного общества, но и к новым социально-политическим условиям с разноплановыми проявлениями конкурентной борьбы.

Информационная безопасность – это защищенность информации от преднамеренных и не преднамеренных атак, взломов, краж данных, включающая в себя методы и особенности обеспечения защиты. [1]

Актуальные виды угроз:

1. Раскрытие закрытой (приватной) информации.
2. Взлом (незаконное вмешательство в работу компьютера).
3. Вывод компьютера из нормального рабочего состояния или значительное понижение его производительности.
4. Превышение прав не привилегированных пользователей.
5. Отказ от авторства и транзакций.
6. Уничтожение и изменение информации.

Рассмотрим один из распространенных видов хакерской атаки, DDoS-атаку. DDoS-атака (от англ. Distributed Denialof Service, Распределённый отказ от обслуживания) это хакерская атака, цель которой это вывести систему из рабочего состояния, либо получить доступ к системе, при которой организуется огромное количество запросов, которые не может обработать система, и будет вынуждена остановиться. В настоящее время DDoS-атаки являются наиболее популярными, так как могут сломать большое количество систем, при этом не оставляя серьезных улик. [2]

Схема DDoS-атаки представлена ниже на рисунке 1.

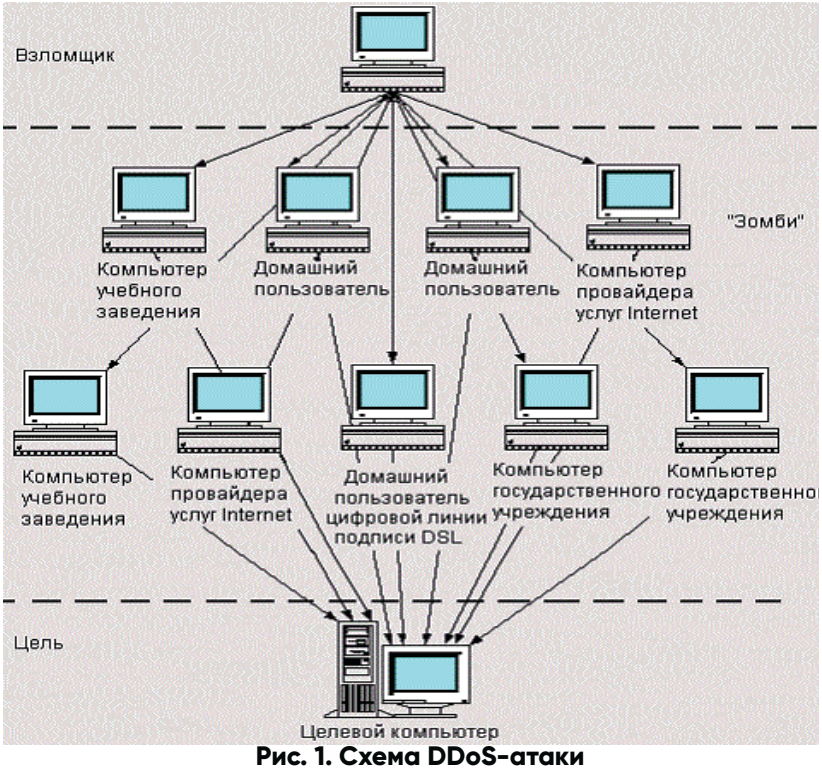

Рис. 1. Схема DDoS-атаки

Рисунок 2. DDoS-атаки по странам

На рисунке 2 представлена статистика по странам, которые подвержены этим атакам.

Причины DDoS-атак: [3]

- Вымогательство
- Личная неприязнь
- Развлечение
- Протест (против действий правительства, корпорацийи т.п.)
- Шантаж
- Конкуренция

Защита от DDoS-атак:

1. Предотвращение (Профилактика причин, из-за которых организовывают DDoS-атаки)
2. Выявление и исключение уязвимостей
3. ПО (постоянное обновление и контроль)
4. Фильтрация и блэкхолин [4] (Блокирование данных, исходящих от системы атакующих)
5. Наращивание ресурсов.
6. Обратный DDoS (Перенаправить трафик атакующего на него же самого)
7. Ответные действия (поиск источника DDoS атак, наказание(предусмотренное законодательством))
8. Децентрализация атаки
9. Избежание атаки с помощью уклонения (Увод цели атаки от других ресурсов, которые подвергаются атаке)
10. Использованиеспецоборудования для отра-

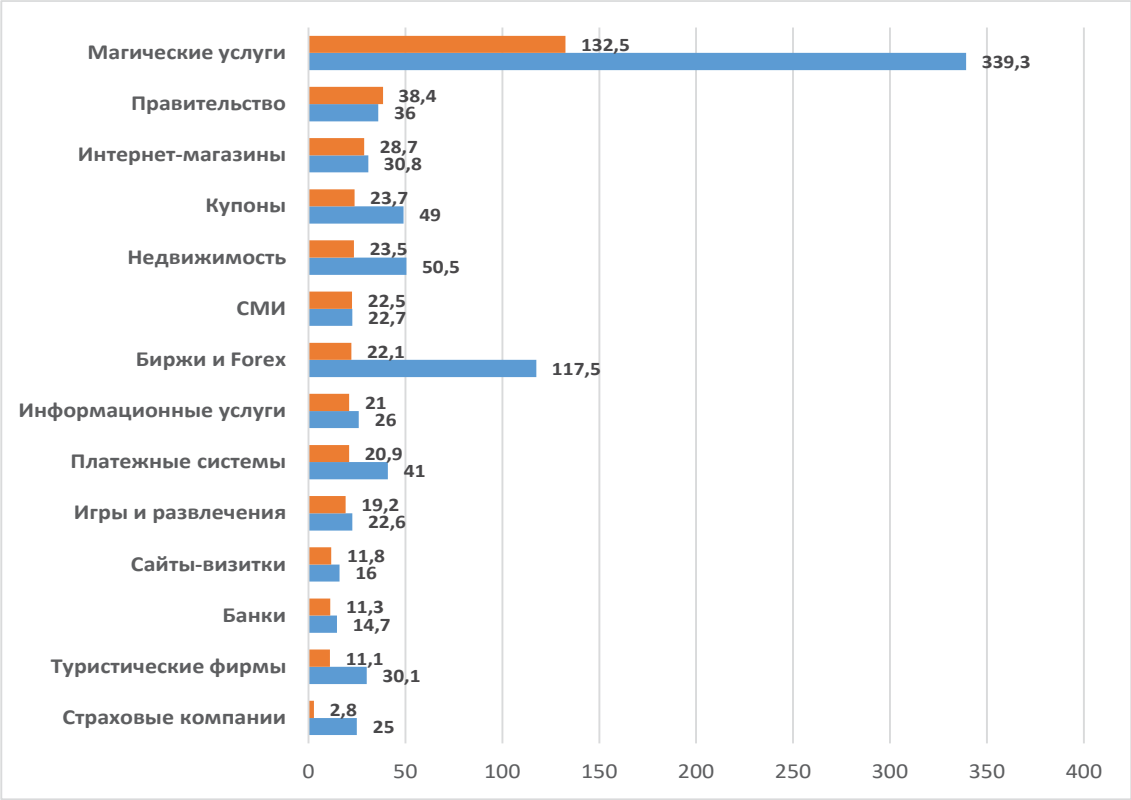

Рисунок 3. Статистика DDoS-атак

жения DDoS-атак.

11. Использование сервисов по защите от DDoS-атак.

По данным «Лаборатории Касперского» число DDoS-атак на компании, находящиеся в России, увеличилось вдвое на момент 2017 года, при этом уже треть компаний (36%) подверглась хотя-бы одной DDoS-атаке. Это показывает исследование по информационной безопасности, проведенное «Лабораторией Касперского», которое производилось среди 5200 IT-специалистов из 29 стран, в том числе и России. Для сравнения, в 2016 году DDoS-атакам вдвое меньше компаний (17%). Из этих цифр видно, что идет тренд на увеличение DDoS-атак. Статистика показала (рисунок 4), что главной мишенью при DDoS-атаках является крупный бизнес – 36%, средний и малый бизнес – 30%, микропредприятия - 34%. Последствия данных атак (рисунок 5) часто оказывались серьезными, 21% пострадавших отметили, что атака привела к снижению производительности сервисов компании, а каждого двенадцатого (8%) произошли сбои с транзакциями. Как показала практика, часто DDoS-атака является лишь прикрытием для совершения других операций злоумышленников. Почти в половине случаев (47%), во время этой атаки производилась кража данных пользователей. В 43% атак, DDoS-атаки являлись прикрытием для взлома корпоративных сетей, а в 41% случаев, атака дополнительно несла в себе заражение компьютерных систем вредоносным ПО.У трети (31%) атакованных зафиксирована кража денег [5]. На состояние 2015 года Россия занимает пятое место DDoS-атакам. Выше находятся следующие страны: Канада, США, Южная Корея, Китай. Атаки же чаще всего проводят российские и китайские хакеры. [6]

Методы защиты информации от возможных угроз:

1. Создание разрешительных систем доступа пользователей.
2. Уменьшение круга пользователей в помещении, в котором расположены носители информации.
3. Создание многоступенчатой системы допуска к информации и воздействиям на неё.
4. Регистрация пользователей для предотвращения изменения информации.
5. Создание копий на иных носителях информации для того, чтобы избежать потери информации.
6. Сохранение охраняемой информации для её дальнейшей обработки.
7. Применение закрытых каналов связи.
8. Организация обработки информации с помощью различных средств защиты.
9. Недопустимость использования вредоносного ПО. [7]

Методы обеспечения информационной безопасности имеют 3 определенных типа:

- Правовые (устранение противоречий в федеральном законодательстве, следование Федеральному закону от 27.07.2006 N 149-ФЗ (ред. от 29.07.2017)) [8]
- Организационно-технические (Улучшение системы обеспечения информационной безопасности, усиление деятельности Органов (в рамках дозволенного Конституцией РФ), улучшение средств защиты информации, повышение надежности специального ПО.)
- Экономические (Финансирование ПО свя-

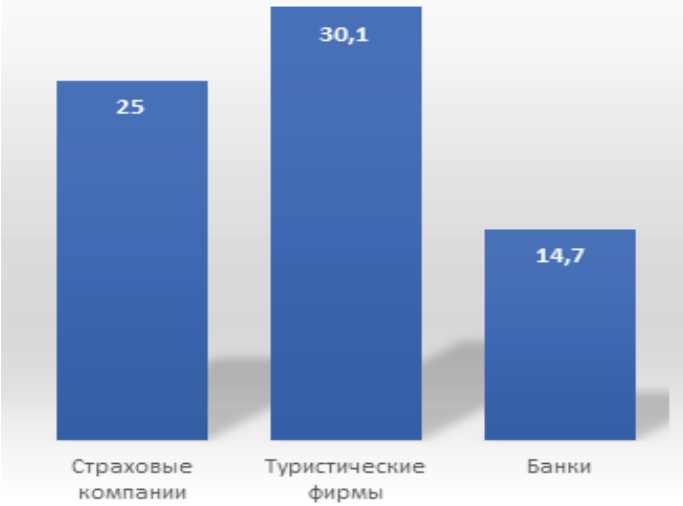

Рисунок 4. Статистика DDoS - атак на предприятия

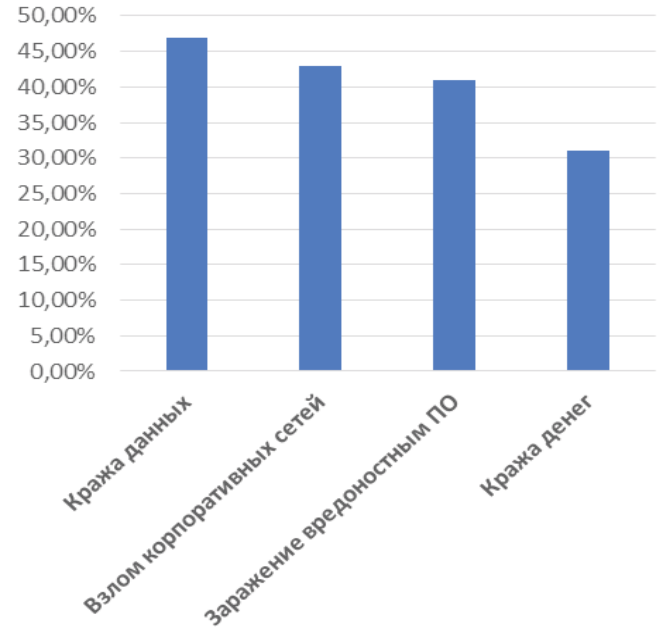

Рисунок 5. Преступления, совершаемые во время DDoS-атак

занного с безопасностью, применение систем страхования информационных рисков.)

Стоит заметить, что на сегодняшний день работа с информацией задействована во всех сферах, будь то работа в банковской сфере, где необходимо отслеживать все изменения на рынке, следить за денежным потоком внутри банка, а также между банками, хранить огромные базы данных о физических, юридических лицах, их вкладах, счетах, будь то образовательная сфера, где нужно владеть огромными базами данных о обучающихся, сотрудниках. Хранить информацию о научно-исследовательской деятельности, литературу, которая может быть задействована при обучении. Иметь данные о финансовой составляющей в образовательном учреждении, как, например, зарплата преподавателей, стипендии и т.д.

Каждая сфера имеет свою специфику и направление, однако, их объединяет то, что они все нуждаются в информационной защите: обойдя систему защиты банка, можно нарушить его деятельность, получив доступ к счетам вкладчиков, тем самым нанести ему крупный материальный и репутационный удар.

Взломав систему защиты университета можно получить персональные данные об обучающихся, сотрудниках. Украсть плоды интеллектуальной деятельности, проводимой там.

Информационная безопасность корпоративных сетей в ВУЗах.

В современном вузе хранится и обрабатывается огромное количество различных данных, связанных не только с обеспечением учебного процесса, но и с научно-исследовательскими и проектно-конструкторскими разработками, персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация. Рост количества преступлений в сфере высоких технологий диктует свои требования к защите ресурсов вычислительных сетей учебных заведений и ставит задачу построения собственной интегрированной системы безопасности. Ее решение предполагает наличие нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации (СЗИ) в рамках образовательного учреждения. Эти составляющие определяют единую политику обеспечения безопасности информации в вузе. Специфика защиты информации в образовательной системе заключается в том, что вуз –публичное заведение с непостоянной аудиторией, а также место повышенной активности «начинающих киберпреступников».

Особенности вуза как объекта информатизации связаны также с многопрофильным характером деятельности, обилием форм и методов учебной работы, пространственной распределенностью инфраструктуры (филиалы, представительства). Сюда же можно отнести и многообразие источников финансирования, наличие развитой структуры вспомогательных подразделений и служб (строительная, производственная, хозяйственная деятельность), необходимость адаптации к меняющемуся рынку образовательных услуг, потребность в анализе рынка труда, отсутствие общепринятой формализации деловых процессов, необходимость электронного взаимодействия с вышестоящими организациями, частое изменение статуса сотрудников и обучаемых. Несколько облегчает проблему то, что вуз представляет собой стабильную, иерархическую по функциям управления систему, обладающую всеми необходимыми условиями жизнедеятельности и действующую на принципах централизованного управления (последнее означает, что в управлении задачами информатизации может активно использоваться административный ресурс).

Указанные выше особенности обусловливают необходимость соблюдения следующих требований:

- комплексная проработка задач информационной безопасности, начиная с концепции

и заканчивая сопровождением программно-технических решений;
- привлечение большого числа специалистов, владеющих содержательной частью деловых процессов;
- использование модульной структуры корпоративных приложений, когда каждый модуль покрывает взаимосвязанную группу деловых процедур или информационных сервисов при обеспечении единых требований к безопасности;
- применение обоснованной последовательности этапов в решении задач информационной безопасности;
- документирование разработок на базе разумного применения стандартов, что гарантирует создание успешной системы;
- использование надежных и масштабируемых аппаратно-программных платформ и технологий различного назначения, обеспечивающих необходимый уровень безопасности.

С точки зрения архитектуры в корпоративной информационной среде можно выделить три уровня, для обеспечения безопасного функционирования которых необходимо применять различные подходы:
- оборудование вычислительной сети, каналов и линий передачи данных, рабочих мест пользователей, системы хранения данных;
- операционные системы, сетевые службы и сервисы по управлению доступом к ресурсам, программное обеспечение среднего слоя;
- прикладное программное обеспечение, информационные сервисы и среды, ориентированные на пользователей.

Предпосылками к появлению корпоративных сетей в ВУЗах является внедрение новых технологий и регулярное использование Интернета в системе управления ВУЗом. Что же представляет из себя корпоративная сеть? Корпоративная сеть - это информационная система, которая включает в себя все виды информационных технологий и информационной деятельности, целью которой является решение задач связанных, непосредственно, с управлением ВУЗом. Корпоративная сеть ВУЗа основана на «скудном финансировании» (техника, нелицензионное ПО). Корпоративная сеть не имеет какой-либо глобальной цели для развития. Корпоративная сеть подразумевает решение 2 основных задач:

1. Обеспечение как научной, так и образовательной видов деятельности.

2. Решение задачи управления как образовательным, так и научным процессами.

В связи с тем, что корпоративные сети изначально создавались для решения разных задач, следует, что корпоративные сети разнородны.

Рубежи защиты

Первым и, пожалуй, немало важным рубежом защиты является роутер. Функции роутера:
- эффективное разделение трафика;
- связывает разные участки сети друг с другом;
- способствует использованию альтернативных путей между узлами сети.

Маршрутизатор позволяет беспрепятственно функционировать различным подсетям и помогает установить связь с глобальными сетями (WAN). Несомненно, главной задачей маршрутизатора является обеспечение безопасности в отказе обслуживания (DDOS).

Вторым рубежом защиты межсетевой экран (МСЭ): аппаратно-программный комплекс CiscoPIXFirewall.

Третьим рубежом защиты демилитаризованная зона (DMZ). Прокси-сервер обрабатывает запросы от рабочих станций учебного персонала, не подключенных напрямую к роутеру. [9]

Вывод:

Информационная безопасность является крайне важным аспектом стабильного существования любой организации.

Следует уделять должное внимание безопасности серверов, спонсировать развитие информационной безопасности. Необходимо придерживаться базовых вещей для безопасности, как минимум, установление антивирусов, регулярной диагностики компьютерных систем.

В каждой компании должны быть сотрудники, которые отвечают за безопасность компьютерных систем, которому необходимо постоянно совершенствовать знания, т.к. эта сфера является крайне изменчивой и обширной.

Тем не менее, даже самая защищенная система имеет одну главную уязвимость – человеческий фактор.

Список литературы:

1. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).
2. Н. Фергюсон, Б. Шнайер. Практическая криптография. — Москва: Вильямс, 2005. — С. 416.
3. Иллюстрированный самоучитель по защите в Интернет. — 2004. — С. 2, 3, 4, 5, 6, 7, 8, 9, 12.
4. S.Agarwal, T. Dawson, C. Tryfonas. DDoS Mitigation via Regional Cleaning Centers. — 2011.
5. ТАСС: «Лаборатория Касперского»: число DDoS-атак на компании из РФ за год выросло в два раза
6. ТАСС: Экономика и бизнес — «Лаборатория Касперского»: каждая шестая компания РФ в 2015 г. подвергалась DDoS-атаке
7. https://securelist.ru, consultant.ru
8. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017)
9. «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2018)
10. Проталинский О.М., Ажмухамедов И.М. «Информационная безопасность. Защита информации".