УДК 004.056

КОМПЛЕКСНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ВУЗЕ

Московский политехнический университет, Москва
Moscow Polytechnic University, Moscow

ТЮМЕНЕВ
Александр Владимирович
Подполковник полиции, начальник управления комплексной безопасности

TYUMENEV Alexander
Lieutenant Colonel of police, head of integrated security

ПАНОВ
Николай Николаевич
Заместитель начальника отдела охраны комплексной безопасности

PANOV Nikolay
The Deputy chief of Department of protection of a comprehensive security

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

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.

COMPREHENSIVE INFORMATION SECURITY AT THE UNIVERSITY

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

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.

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. 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 [1].

В настоящее время DDoS-атаки являются наиболее популярными, так как могут сломать большое количество систем, при этом не оставляя серьезных улик [2].

По данным «Лаборатории Касперского» число DDoS-атак на компании, находящиеся в России, увеличилось вдвое (на период 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 подвергались вдвое меньше компаний

(17%). Из этих цифр видно, что идет тренд на увеличение DDoS-атак. Статистика показала (Рисунок 1), что главной мишенью при DDoS-атаках является крупный бизнес – 36%, средний и малый бизнес – 30%, микропредприятия – 34%. Последствия данных атак (Рисунок 2) часто оказывались серьезными, 21% пострадавших отметили, что атака привела к снижению производительности сервисов компании, а у 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% 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]. По состоянию на 2015 год Россия занимает пятое место по DDoS-атакам. Выше находятся следующие страны: Канада, США, Южная Корея, Китай. Атаки же чаще всего проводят российские и китайские хакеры [3].

Методы обеспечения информационной безопасности имеют 3 определенных типа:

1. Правовые (устранение противоречий в федеральном законодательстве, следование Федеральному закону от 27.07.2006 N 149-ФЗ (ред. от 29.07.2017)) [4].

2. Организационно-технические (Улучшение системы обеспечения информационной безопасности, усиление деятельности Органов (в рамках дозволенного Конституцией РФ), улучшение средств защиты информации, повышение надежности специального ПО).

3. Экономические (Финансирование ПО связанного с безопасностью, применение систем страхования информационных рисков).

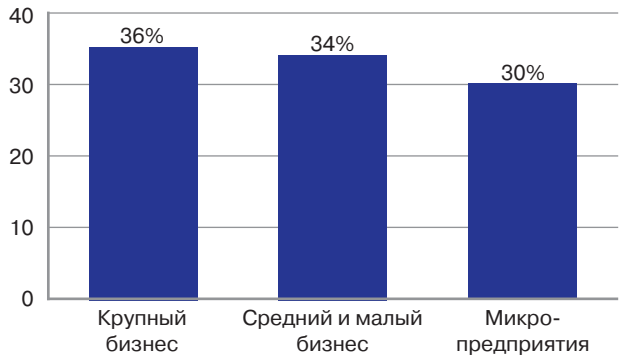

Рисунок 1 – Статистика DDoS-атак на предприятия

Стоит заметить, что на сегодняшний день работа с информацией задействована во всех сферах. Образовательная сфера, где нужно владеть огромными базами данных об 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.

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

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,

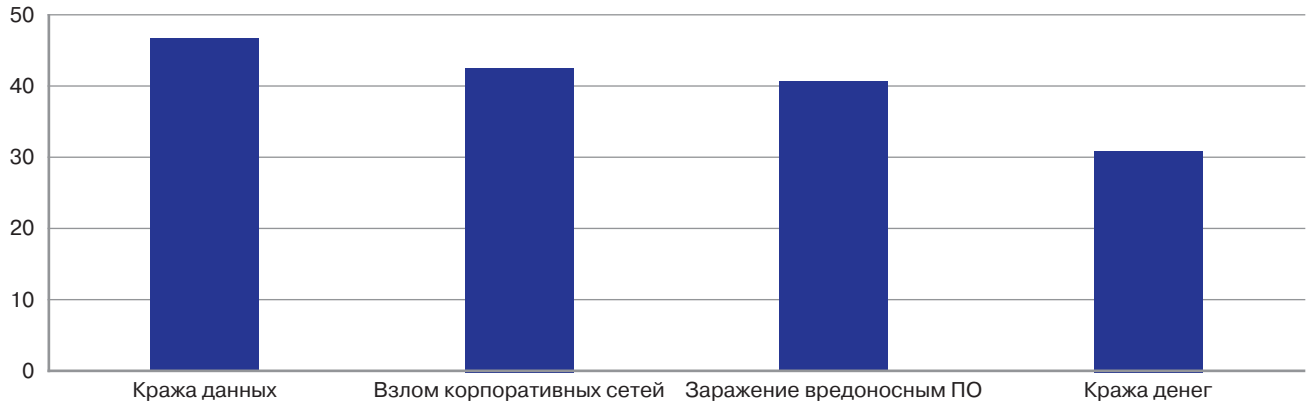

Рисунок 2 – Преступления, совершаемые во время DDoS-атак

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:

– комплексной проработки задач информационной безопасности, начиная с концепции и заканчивая сопровождением программно-технических решений;

– привлечения большого числа специалистов, владеющих содержательной частью деловых процессов;

– использования модульной структуры корпоративных приложений, когда каждый модуль покрывает взаимосвязанную группу деловых процедур или информационных сервисов при обеспечении единых требований к безопасности;

– применения обоснованной последовательности этапов в решении задач информационной безопасности;

– документирования разработок на базе разумного применения стандартов, что гарантирует создание успешной системы;

– использования 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. 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.

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.

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

Литература

1. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006, – Введ. 2008–02–01).

2. ТАСС: «Лаборатория Касперского»: число DDoS-атак на компании из РФ за год выросло в два раза.

3. Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 № 149-ФЗ (последняя редакция) : [принят Гос. Думой 8 июля 2006 г.: одобр Советом Федерации 14 июля 2006 г.].

4. Байковский, Ю.В. Факторы, определяющие экстремальность спортивной деятельности / Ю.В. Байковский // Экстремальная деятельность человека. – 2016. – № 2 (39). – С. 55-59.

5. Гарбузюк, И.В. Анализ рисков инновационных проектов / И.В. Гарбузюк, Е.О. Бузина // В сборнике: Современные тенденции развития науки и образования: Теория и практика Материалы 1 Международной научно-практической конференции научно-педагогических работников и молодых ученых; под ред. Г.С. Жуковой, В.В. Бритвиной, 2017. – С. 89-96.

6. Тюменев, А.В. Обеспечение безопасности информационных ресурсов предприятия / А.В Тюменев, Н.Н. Панов // Системные технологии. – 2017. – № 3 (24).– С. 68-71.

7. Бритвина, В.В. Гимнастические упражнения с силовым компонентом для лиц, занимающихся экстремальными видами деятельности, перенесших инфаркт миокарда / В.В. Бритвина // Теория и практика прикладных и экстремальных видов спорта. – 2012. – № 1 (23). – С. 50-52.

8. Панов, Н.Н. Сравнительный анализ безопасного вида транспорта в россии / Н.Н. Панов, А.В. Тюменев // Системные технологии. – 2017. – № 3 (24). – С. 34-39.

9. Жилкова, Ю.В. Кластерный подход в туризме / Ю.В. Жилкова, З.В Макаренко, Г.П. Конюхова, В.Г. Конюхов, В.В. Бритвина, Н.В. Шабалина // Теория и практика прикладных и экстремальных видов спорта. – 2012. – № 3 (25). – С. 49-51.

10. Панов, Н.Н. Сравнительный анализ причин ДТП в трех странах: Германии, США и России / Н.Н. Панов, Э.С. Цыганков, В.Н. Зудин, В.В. Бритвина, В.Г. Конюхов // Экстремальная деятельность человека. – 2016. – № 2 (39). – С. 19-24.

11. Панов, Н.Н. Статистический анализ дорожно-транспортных происшествий происходящих по вине пешеходов в россии / Н.Н. Панов., В.Н. Зудин, В.Г. Конюхов, В.В. Бритвина // Экстремальная деятельность человека. – 2016. – № 3 (40). – С. 58-62.

12. S. Agarwal, T. Dawson, C. Tryfonas. DDoS Mitigation via Regional Cleaning Centers. – 2011.

Literature

1. The national standard of the Russian Federation «Information protection. Basic terms and definitions «(GOST R 50922-2006).

2. TASS: «Kaspersky Lab»: the number of DDoS attacks on companies from Russia for the year increased twice.

3. Federal Law of July 27, 2006 N 149-FZ (as amended on November 25, 2017).

4. Baikovskiy, Yu.V. Factors determining the extremity of sports activity / Yu.V. Baikovskiy // Extreme activity of man. – 2016. – No. 2 (39). – P. 55-59.

5. Garbuzyuk, I.V. Analysis of risks of innovative projects / I.V. Garbuzyuk, E.O. Buzina // In the collection: Current Trends in the Development of Science and Education: Theory and Practice Materials of the 1 International Scientific and Practical Conference of Scientific Pedagogical Workers and Young Scientists; Ed. G.S. Zhukova, V.V. Britvina, 2017. – P. 89-96.

6. Tyumenev, A.V. Ensuring the security of information resources of the enterprise / A.V. Tyumenyev, N.N. Panov // System technologies. – 2017. – No. 3 (24). – P. 68-71.

7. Britvina, V.V. Gymnastic exercises with a force component for people engaged in extreme activities that have suffered myocardial infarction / V.V. Britvina // Theory and Practice of Applied and Extreme Sports. – 2012. – No. 1 (23). – P. 50-52.

8. Panov, N.N. Comparative analysis of the safe mode of transport in Russia / N.N. Panov, A.V. Tyumen // System technologies. – 2017. – No. 3 (24). – P. 34-39.

9. Zhilkova, Yu.V. Cluster approach in tourism / Yu.V. Zhilkova, Z. Makarenko, G.P. Konyukhova, V.G. Konyukhov, V.V. Britvina, N.V. Shabalin // Theory and practice of applied and extreme sports. – 2012. – No. 3 (25). – P. 49-51.

10. Panov, N.N. Comparative analysis of the causes of accidents in three countries: Germany, the USA and Russia / N.N. Panov, E.S. Tsygankov, V.N. Zudin, V.V. Britvina, V.G. Konyukhov // Extreme human activity. – 2016. – No. 2 (39). – P. 19-24.

11. Panov, N.N. Statistical analysis of road accidents caused by pedestrians in Russia / N.N. Panov., V.N. Zudin, V.G. Konyukhov, V.V. Britvina // Extreme human activity. – 2016. – No. 3 (40). – P. 58-62.

12. S. Agarwal, T. Dawson, C. Tryfonas. DDoS Mitigation via Regional Cleaning Centers. – 2011.