Тюменев А.В.

§3.7. Технические решения и информационные технологии в обеспечении безопасности вуза.

Проанализирована информационная безопасность корпоративных сетей в ВУЗах. Рассмотрены методы обеспечения информационной безопасности, а так же разработаны требования позволявшие обеспечить информационную безопасность в ВУЗах. Сделан вывод об информационной безопасности, которая является крайне важным аспектом стабильного существования любой организации.

Ключевые слова: Информационные технологии, безопасность вуза, корпоративные сети.

Tyumenev A.V.

§3.7. Technical solutions and information technology to ensure the safety of the university.

Analyzed the information security of corporate networks in universities. Methods for ensuring information security are considered, as well as requirements have been developed to ensure information security in universities. The conclusion is made about information security, which is an extremely important aspect of the stable existence of any organization.

Keywords: Information technology, university security, corporate networks.

Актуальность проблемы обеспечения комплексной безопасности образовательных организаций в современном мире обусловлена необходимостью создания условий для развития личности, приобретения знаний, умений, навыков и формирования компетенций, необходимых для выполнения трудовой, служебной деятельности и продиктована Федеральным законом « Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ (ред. от 03.02.2014)[1]

[1] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2018)

Обеспечение безопасности студенческой молодежи, находящихся в образовательных учреждениях признано одним из важнейших направлений работы руководства страны и системы образования. Как отметил Президент России, "техническое состояние зданий, пожарная безопасность, обеспечение пропускного режима - все это должно быть в зоне постоянного внимания соответствующих структур, тех, кто отвечает за безопасность, и они же должны нести за это прямую ответственность, юридическую ответственность"

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 [5].

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

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 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 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. На состояние 2017 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. [3]

Рисунок 1. Статистика DDoS - атак на предприятия.

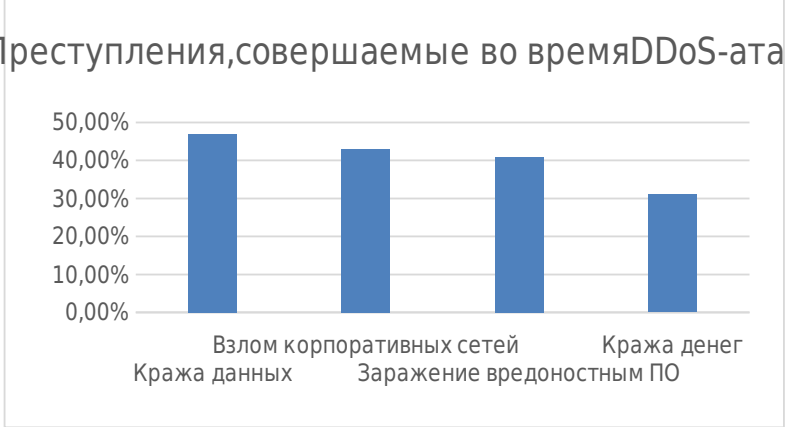

Рисунок 2. Преступления, совершаемые во время DDoS-атак.

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)) [4]
- -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 связанного с безопасностью, применение систем страхования информационных рисков.)

Стоит заметить, что на сегодняшний день работа с информацией задействована во всех сферах. 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.

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

деятельности, проводимой там.

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 [6]. 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.

В связи с тем, что корпоративные сети изначально создавались для

решения разных задач, следует, что корпоративные сети разнородны.

Рубежи защиты:

1. Первым 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). Главной задачей маршрутизатора является обеспечение безопасности в отказе обслуживания (DDOS).

1. Вторым рубежом защиты межсетевой экран (МСЭ): аппаратно-программный комплекс CiscoPIXFirewall.
2. Третьим рубежом защиты демилитаризованная зона (DMZ). Прокси-сервер обрабатывает запросы от рабочих станций учебного персонала, не подключенных напрямую к роутеру.

Вывод. 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.

Информационная безопасность является важным аспектом стабильного существования любой организации, и в частности вуза.

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

В каждом Вузе должны быть сотрудники, которые отвечают за безопасность компьютерных систем, которому необходимо постоянно

совершенствовать знания, т.к. эта сфера является крайне изменчивой и обширной.

Целью системы обеспечения безопасности участников образовательного процесса является сохранение жизни и здоровья учащихся и работников образовательных учреждений.

Библиографический список

1. Радиков И. В. Национальная безопасность как главный национальный проект России: типичные проблемы реализации //Радиков И. В. Политическая экспертиза: Политэкс. Научный журнал. Том3. № 1. СПб.: Изд-во С.-Петерб. ун-та, 2007, С.64–81.

2. Ковалев А. А. Роль информационных технологии в обеспечении безопасности государства // Молодой ученый. — 2016. — №21. — С. 767-771.

3. ТАСС:"Лаборатория Касперского": число DDoS-атак на компании из РФ за год выросло в два раза

4. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.01.2018)

5. Молчанов И.Н., Холдеев К.А. Социально ответственный бизнес: поддержка образовательных проектов // В сб.: Россия: тенденции и перспективы развития. Ежегодник. Отв. ред. В.И. Герасимов. М., 2017. С. 565-569.

6. Молчанов И.Н., Титова А.И. Информатизация как фактор повышения качества предоставления государственных услуг // В сб.: Россия: тенденции и перспективы развития. Ежегодник. Отв. ред. В.И. Герасимов. М., 2017. С. 620-624.