Угрозы в области хранения данных

В.М. Курейчик, О.Н. Сахарова, С.С. Пирожков

Южный федеральный университет, Таганрог

Аннотация: В настоящий момент в условиях активно развивающегося информационного общества информация становится необходимым фактором производства, поэтому обеспечение сохранности данных является важным вопросом. Статья посвящена актуальным, на сегодняшний день, проблемам, связанным с угрозами в области хранения данных. Дано определение понятию угрозы в области хранения данных; предложена классификация по видам угроз; выделены следующие классы угроз в области хранения данных: пространственная, коммуникативная, деструктивная; описаны фактические составляющие угроз. На основе проведенного анализа угроз в области хранения данных будут в дальнейшем разработаны алгоритмы обеспечения сохранности информации.
Ключевые слова: информация, данные, хранение данных, сохранность данных, целостность данных, угрозы хранения данных, угрозы целостности данных.
.

Введение

В условиях активно развивающегося информационного общества информация становится необходимым фактором производства, которая имеет как физическую, так и материальную ценность. Обеспечение сохранности данных является важнейшим аспектом при работе с информацией не только в локальных сетях, но и в глобальной сети Интернет. Если для физических лиц хранимая информация имеет личную ценность, и утрата таких данных может принести эмоциональный дискомфорт, то для юридических лиц потеря или нарушение целостности информации может привести к серьёзным финансовым убыткам. Поэтому обеспечение сохранности данных будет являться актуальным вопросом до тех пора пока она представляет собой ценность.

Под угрозами в области хранения данных понимается частичная или полная потеря данных, а также отсутствие доступа к ним.

В настоящий момент существует масса угроз, в том числе и при работе в Интернет, которые влекут за собой не только частичное повреждение, но и полное удаление данных. Для организации правильного хранения и защиты

информации необходимо провести анализ и систематизацию существующих угроз, что позволит сформировать алгоритмы обеспечения сохранности информации [1].

Анализ угроз в области хранения данных

Анализируя все существующие на сегодняшний день угрозы в области хранения данных, можно выделить следующие базовые классы:

1) Пространственная угроза: Нехватка физического пространства для хранения информации;
2) Коммуникативная угроза: Отсутствие доступа к информации;
3) Деструктивная угроза: Потеря данных.

Рис.1. – Классификация угроз

Рассмотрим более подробно каждый из выделенных базовых классов угроз в области хранения данных.

Пространственная угроза

Пространственная угроза – это угроза, возникающая в результате переполнения хранилища данными вследствие постоянно растущего объема сохраняемых данных.

Таким образом, можно выделить три уровня пространственных угроз:

1) персональная пространственная угроза;
2) серверная пространственная угроза;
3) «облачная» или глобальная пространственная угроза.

Персональная пространственная угроза возникает при работе на отдельно стоящей рабочей станции в результате постоянного увеличения хранимой информации. Вследствие этого рано или поздно наступает момент, когда дальнейшее накопление информации становится невозможным из-за физического отсутствия места на устройствах хранения информации [2]. Для устранения этой угрозы существуют следующие пути:

1) увеличение внутреннего объёма для хранения информации за счёт либо увеличения количества устройств хранения информации, либо за счёт замены устройства хранения информации на устройство с большим объёмом памяти;

2) использование внешних устройств хранения информации, что подразумевает под собой частичный или полный перенос хранимой информации на локальный сервер или в облако.

Серверная пространственная угроза возникает, как правило, в организациях в результате нехватки места для хранения информации на сервере. Пути решения серверной пространственной угрозы фактически идентичны способам устранения персональной пространственной угрозы и отличаются лишь масштабами, то есть:

1) увеличение внутреннего объёма сервера для хранения информации за счёт либо увеличения количества устройств хранения информации, либо за счёт замены устройства хранения информации на устройство с большим объёмом памяти;

2) использование внешних устройств хранения информации, что подразумевает под собой частичный или полный перенос хранимой информации в облако.

Облачная или глобальная пространственная угроза возникает в результате переполнения всех имеющихся облачных хранилищ данных. В настоящее время уровень развития современных облачных технологий

ориентирован на петабайтные наборы объема данных и гигабайтные потоки данных, что в достаточной степени обеспечивает возрастающие с каждым днём потребности в хранении данных [3]. Однако, поскольку объёмы информации, в отличии от объёмов хранилищ данных, растут нелинейно, то может наступить момент, когда объёма облачных хранилищ данных будет недостаточно.

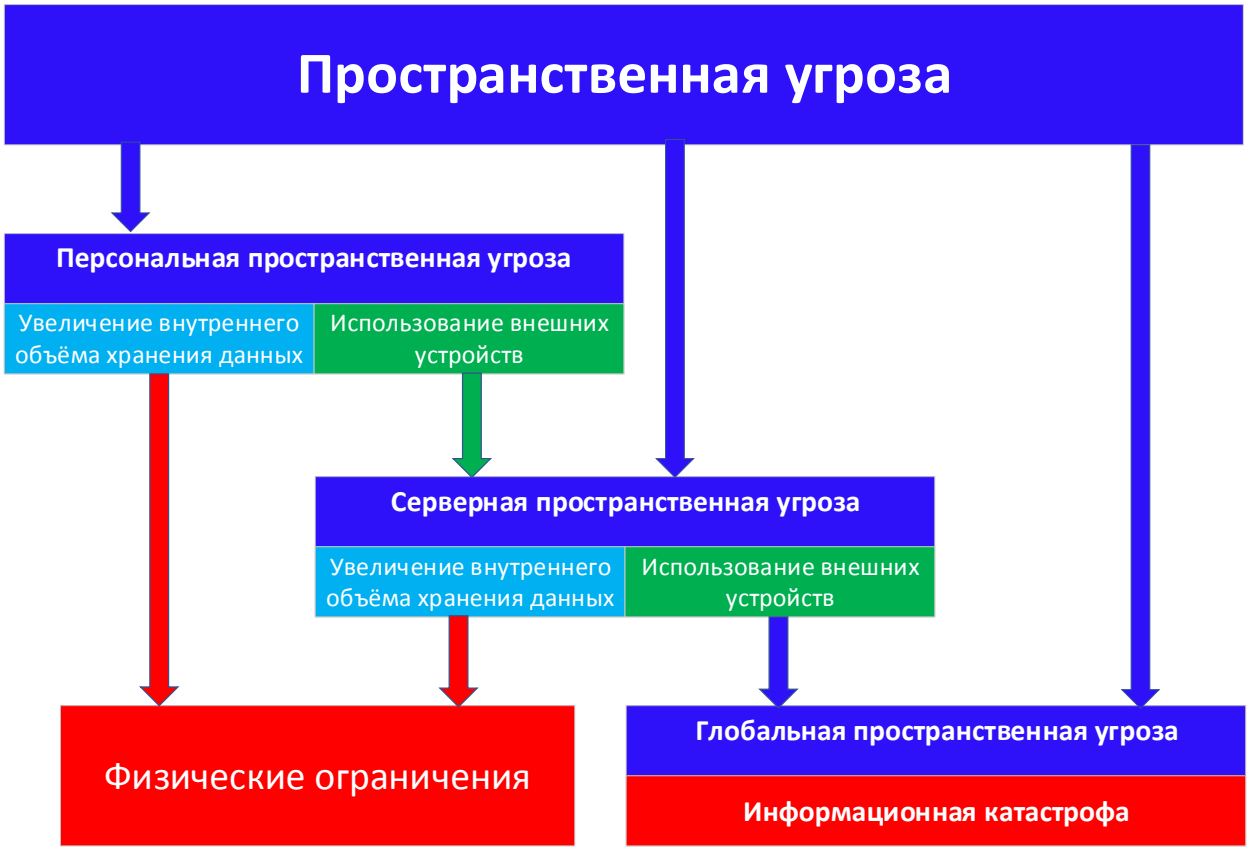

Рис. 2. – Уровни пространственной угрозы

Анализируя возникающие пространственные угрозы в обеспечении сохранности информации, можно сделать следующий вывод. Для устранения персональной пространственной угрозы один из путей – использование серверных хранилищ данных, в результате чего может произойти их переполнение и, как следствие, возникает серверная пространственная угроза. Один из способов устранения серверной пространственной угрозы – хранение данных в облаке, что, в свою очередь, приводит к потенциальной

глобальной пространственной угрозе [4]. Таким образом получается, что использование внешних устройств хранения информации для устранения всех уровней пространственных угроз рано или поздно могут привести к глобальной пространственной угрозе и информационной катастрофе. Тогда, напрашивается вывод, что перспективный способ решения пространственных угроз – это наращивание внутренних объёмов хранения информации. Однако, такой подход, в свою очередь, ограничен физическими возможностями используемых устройств. Следовательно, единственный правильный путь устранения пространственной угрозы – это систематический анализ объёмов используемых накопителей и комбинирование способов хранения.

Коммуникативная угроза

Коммуникативная угроза - это угроза, возникающая в результате отсутствия доступа к данным.

Наиболее актуальна коммуникативная угроза для компаний, ресурсы которых обязаны функционировать в бесперебойном режиме круглосуточно (24/7) – это банки, крупные сети розничной торговли (ритейл), телекоммуникационные операторы и др. Для этих организаций каждая минута «простоя» влечёт большие финансовые потери и может нанести урон престижу. По результатам исследования компании, специализирующейся в области решений для резервного копирования и управления данными в облаке, (Veeam Software) за 2019 год 73% компаний подтверждают, что не в состоянии обеспечить своим клиентам стабильный бесперебойный доступ к информации, продуктам и услугам, и на этом компании теряют в среднем по $20 миллионов ежегодно [5].

Таким образом, можно выделить следующие типы коммуникативных угроз:

1) техническая коммуникативная угроза;

2) физическая коммуникативная угроза.

Техническая коммуникативная угроза возникает в результате выхода из строя оборудования, либо в результате производственного брака, либо в результате нарушений условий эксплуатации.

Под оборудованием, в данном случае, понимается не только серверные платформы, на которых хранится информация, но и коммутационное оборудование, обеспечивающее связь, и пользовательские устройства: персональные компьютеры, ноутбуки, автоматизированные рабочие места, графические станции, терминалы тонких клиентов и т.д. [6].

Следовательно, техническая коммуникативная угроза может быть разделена на следующие виды:

1) клиентская техническая коммуникативная угроза;
2) провайдерская техническая коммуникативная угроза;
3) сервисная техническая коммуникативная угроза.

Клиентская техническая коммуникативная угроза возникает в результате выхода из строя оборудования на стороне пользователя.

Провайдерская техническая коммуникативная угроза возникает в результате выхода из строя оборудования на стороне провайдера (компании, предоставляющей доступ в интернет) [7].

Сервисная техническая коммуникативная угроза возникает в результате выхода из строя оборудования на стороне компаний, предоставляющей услуги по хранению данных (виртуальных хостинги, облачные хранилища и т.д.).

Физическая коммуникативная угроза возникает в результате проблем с линиями коммутации.

На сегодняшний день, даже в передовых странах, скорость доступа к сети «интернет» измеряется мегабайтами в секунду. И, несмотря на активное развитие беспроводных технологий, в подавляющем большинстве случаев,

«точечное» подключение к «Интернет» осуществляется через «провод»: по витой паре или оптоволоконному кабелю. Оценить вероятность обрыва кабеля, как из-за человеческого фактора, так и из-за внешних условий или катаклизмов достаточно проблематично [8].

Рис. 3. – Типы коммуникативной угрозы

Также следует учесть ситуацию с отсутствием электропитания на коммутационных устройствах (не всегда заряда источников бесперебойного питания хватает на время, в течение которого возобновляется подача электроэнергии).

Анализируя способы устранения и предотвращения возникновения коммуникативной угрозы, можно сделать вывод о том, что, компания должны заблаговременно проводить профилактику оборудования, иметь в наличии резервные источники питания и резервные линии коммутации.

Деструктивная угроза

Деструктивная угроза – это угроза, которая возникает вследствие внешнего воздействия на данные, в результате чего происходит частичная или полная потеря информации.

Деструктивные угрозы, из-за которых происходит потеря данных, можно разделить на следующие типы:

1) пользовательская деструктивная угроза возникает вследствие ошибки пользователя или оператора, в результате чего данные удаляются ввиду невнимательности или неверно принятых решений;

2) программная (или software-) деструктивная угроза возникает вследствие сбоя в работе системы или программы, приводящего к повреждению или полному удалению данных, в результате чего работать с информацией становится невозможно.

Сбои в работе системы или программы могут произойти в результате отключение электричества, выхода из строя какого-либо физического компонента компьютерной системы в целом, ошибки или недоработки разработчиков программного обеспечения;

3) вирусная деструктивная угроза – это угроза, которая возникает в результате проникновения в систему вируса или вредоносной программы, которые могут стать как причиной повреждения или удаления файлов с жесткого диска, так и изменения данных в нем.

По данным, опубликованным «лабораторией Касперского» за 2019 год:

- в течение года 19,8% компьютеров интернет-пользователей в мире хотя бы один раз подверглись веб-атаке класса Malware;

- решения «Лаборатории Касперского» отразили 975 491 360 атак, которые проводились с интернет-ресурсов, размещенных в различных странах мира;

- зафиксировано 273 782 113 уникальных URL, на которых происходило срабатывание веб-антивируса;

- веб-антивирус Касперского заблокировал 24 610 126 уникальных вредоносных объектов;

4) деструктивная угроза шифрования данных представляет собой разновидность вирусной деструктивной угрозы, поскольку имеет одинаковые способы проникновения в систему. Однако, концептуально деструктивная угроза шифрования данных выделена в отдельный тип, поскольку данные в результате воздействия вируса не удаляются или портятся, а шифруются, с целью последующей коммерческой продажи алгоритмов дешифрования, что фактически является финансовым кибер-преступлением [9].

Последние годы в компаниях проблема с, так называемыми, вирусами-шифровальщиками резко возросла. Их задача - максимально зашифровывать содержимое жесткого диска, и если компьютер подключен к локальной сети, то шифрованию подвергаются все открытые ресурсы на компьютерах в локальной сети и серверах организации. После такой «атаки» пользователи не смогут использовать информацию с компьютеров или серверов до тех пор, пока «авторы» шифровальщика не получат «компенсацию» за расшифровку данных и не предоставят алгоритмы дешифрования данных. Однако, как показывает практика, даже когда произведена «оплата», с огромной вероятностью алгоритмы дешифрования данных не будут предоставлены и информация будет утеряна [10].

Для вирусной деструктивной угрозы и деструктивной угрозы шифрования данных можно выделить следующие пути заражения:

а) подключение внешнего носителя информации (когда вирус проникает в систему при подключении к компьютеру внешних устройств хранения данных);

б) подключение к сети интернет (когда вирус проникает в устройство через скачанный зараженный файл, посещение зараженного сайта, открытие письма с вирусом в электронной почте);

5) хакерская деструктивная угроза – это угроза, которая представляет собой преднамеренное проникновение в компьютерную систему с целью незаконного получения информации, а также повреждения или полного удаления данных.

В официальном ежегодном отчете о киберпреступности (ACR) за 2019 год, опубликованном Cybersecurity Ventures, говорится, что атаки хакеров во всём мире происходят каждые 14 секунд, а к 2021 году их частота возрастёт до каждой 11 секунды;

6) физическая (или hardware-) деструктивная угроза представляет собой угрозу выхода из строя как самого внутреннего устройства хранения информации, так и любого компонента компьютера, нарушение работоспособности которого может привести к выходу из строя внутреннего устройства хранения информации, вследствие чего происходит частичная или полная потеря данных.

На сегодняшний день, деструктивная угроза представляет собой наибольшую опасность для хранения данных, поскольку спрогнозировать её достаточно сложно. Возникновение пространственных угроз при регулярном системном анализе способов хранения данных можно предвидеть. Коммуникативные угрозы не приводят к потере данных, а лишь временно ограничивают доступ к ним. В то же время, предугадать поведение пользователя, сбой в работе системы, несанкционированное проникновение и выход из строя оборудования практически невозможно. Также антивирусное программное обеспечение не даёт стопроцентной гарантии защищенности данных. Однако, правильно организованное резервное копирование данных

позволяет минимизировать последствия возникающих деструктивных угроз [11].

Рис. 4. – Типы деструктивной угрозы

В то же самое время, создание резервных копий требует наличия свободного пространства в устройствах хранения информации, заполнение которого может привести к возникновению пространственной угрозы [12].

Таким образом напрашивается вывод о неизбежности глобальной информационной катастрофы, связанной с отсутствием пространства для хранения информации, для предотвращения которой необходимо четкое представление о понятии угрозы хранения данных и её видах.

Заключение

В данной статье даётся определение понятия угрозы хранения информации, описаны виды, уровни и типы угроз. Пространственная угроза, связанная с отсутствие места хранения данных, может быть предотвращена путём регулярного системного анализа объёмов хранимой информации и использования комбинированных способов её хранения. Коммуникативная угроза, связанная с отсутствием доступа к данным, может быть

предотвращена путем регулярного обслуживания коммутационного оборудования и наличием резервных коммутационных линий связи. Последствия деструктивных угроз, связанных с внешними воздействиями на данные, приводящими к частичной или полной потере данных, могут быть минимизированы путем правильной организации резервного копирования информации [13]. Проведённый анализ угроз в области хранения и защиты данных позволит в дальнейшем сформировать алгоритмы обеспечения сохранности информации, с учётом цикличности возникновения различных видов угроз.

Литература

1. Курейчик В.М., Пирожков С.С. Обзор: Проблемы хранения больших данных // Труды Международного научно-технического конгресса «Интеллектуальные системы и информационные технологии - 2020». – Том №1. С. 420-426.

2. Зараковский Г.М., Смолян Г.Л. Информационно-психологическая безопасность: основные понятия // Психология и безопасность организаций: Сб. науч. тр. / Под ред. Брушлинского А. В. и Лепского В. Е. — М., 1997.

3. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. Санкт-Петербург: Питер, 2020. 1008 с.

4. Абраров, Р. Д. Информационная безопасность в компьютерных сетях // Молодой ученый. 2016. № 9.5 (113.5). С. 10-12. URL: moluch.ru/archive/113/29719/

5. Алексеева М. С. Угрозы безопасности локальных вычислительных сетей // Молодой ученый. 2014. № 18 (77). С. 212-213. URL: moluch.ru/archive/77/13449/

6. Варлатая С. К., Шаханова М. В. Защита информационных процессов в компьютерных сетях. Учебно-методический комплекс. М.: Проспект, 2015. 216с.

7. Басканов А.Н. Способы противодействия и средства раннего выявления DDos-атак // Экономика и качество систем связи. Международный научно-практический электронный журнал. 2019. №3. С.68-76. URL: cyberleninka.ru/article/n/sposoby-protivodeystviya-i-sredstva-rannegovyyavleniya-ddos-atak/viewer

8. A Taxonomy of DDoSW Attacks and DDoS Defense Mechanism – UCLA CSD Thechnical Report no. 020018. URL: lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf

9. Жданова И.В., Быков Д.В. Варианты построения системы защиты электронных документов от копирования // Инженерный вестник Дона, 2012, №2. URL: ivdon.ru/ru/magazine/archive/n2y2012/825

10. Панов Р.И. Современные методы защиты информации на примере российского устройства // Современные проблемы науки и образования, 2015, № 2-2. URL: science-education.ru/ru/article/view?id=23134

11. Enikeeva L.A., Stelmashonok E.V., Stelmashonok V.L. Modeling of information protection system of business processes infrastructure on an industrial plant // International business management, 2016, №3. pp. 315-319.

12.Mingaleva Z., Mirskikh I. Small innovative enterprise: the problems of protection of commercial confidential information and know-how // Middle east journal of scientific research, 2013, №13. С.97-101.

13. Onyigwang J., Shestak Y., Oksiuk A. Information protection of data processing center against cyber attacks // Proceedings of the 2016 IEEE 1st international conference on data stream mining and processing, DSMP 2016, 2016. pp.397-400.

References

1. Kurejchik V.M., Pirozhkov S.S. Trudy` Mezhdunarodnogo nauchno-texnicheskogo kongressa «Intellektual`ny`e sistemy` i informacionny`e texnologii - 2020». Tom №1. pp. 420-426.

2. Zarakovskij G.M., Smolyan G.L. Psixologiya i bezopasnost` organizacij: Sb. nauch. tr. Pod red. Brushlinskogo A. V. i Lepskogo V. E. M., 1997.

3. Olifer V. G., Olifer N. A. Komp`yuterny`e seti. Principy`, texnologii, protokoly`. [Computer networks. Principles, technologies, protocols]. Sankt-Peterburg: Piter, 2020. 1008 p.

4. Abrarov, R. D. Molodoj ucheny`j. 2016. № 9.5 (113.5). pp. 10-12. URL: moluch.ru/archive/113/29719/

5. Alekseeva M. S. Molodoj ucheny`j. 2014. № 18 (77). pp. 212-213. URL: moluch.ru/archive/77/13449/

6. Varlataya S. K., Shaxanova M. V. Zashhita informacionny`x processov v komp`yuterny`x setyax. Uchebno-metodicheskij kompleks. [Protection of information processes in computer networks]. Training and metodology complex. M.: Prospekt, 2015. 216 p.

7. Baskanov A.N. E`konomika i kachestvo sistem svyazi. Mezhdunarodnyj nauchno-prakticheskij elektronnyj zhurnal. 2019. №3. Pp .68-76. URL: cyberleninka.ru/article/n/sposoby-protivodeystviya-i-sredstva-rannego-vyyavleniya-ddos-atak/viewer

8. A Taxonomy of DDoSW Attacks and DDoS Defense Mechanism – UCLA CSD Thechnical Report № 020018. URL: lasr.cs.u cla.edu/ddos/ucla_tech_report_020018.pdf

9. Zhdanova I.V., By`kov D.V. Inzhenernyj vestnik Dona, 2012, №2. URL: ivdon.ru/ru/magazine/archive/n2y2012/825

10. Panov R.I. Sovremenny`e problemy` nauki i obrazovaniya, 2015, № 2-2. URL: science-education.ru/ru/article/view?id=23134

11. Enikeeva L.A., Stelmashonok E.V., Stelmashonok V.L. International business management, 2016, №3. pp.315-319.

12. Mingaleva Z., Mirskikh I. Middle east journal of scientific research, 2013, №13. pp.97-101.

13. Onyigwang o.J., Shestak Y., Oksiuk A. Proceedings of the 2016 IEEE 1st international conference on data stream mining and processing, DSMP 2016, 2016. pp.397-400.