DOI: 10.58168/PPSPM2025_268-272
УДК 004.9

ПРИЧИНЫ ПОТЕРИ ДАННЫХ, МЕТОДЫ БОРЬБЫ И ПРОФИЛАКТИКИ

А.О. Карташов

ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. Работа с большими объемами информации всегда сопряжена с рисками. Ключевым риском в таком случае является потеря данных в силу разных обстоятельств. Понимание причин таких событий может помочь как компаниям, так и отдельным пользователям, выявлять потенциально опасные ситуации и по возможности избегать их.

Ключевые слова: вредоносное ПО, резервные копии, хранение данных, облачное хранилище, восстановление данных.

CAUSES OF DATA LOSS, TREATMENT AND PREVENTION METHODS

A.O. Kartashov

Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. Working with large amounts of information always comes with risks. The key risk in this case is the loss of data due to various circumstances. Understanding the causes of such events can help both companies and individual users identify potentially dangerous situations and avoid them as much as possible.

Keywords: malware, backups, data storage, cloud storage, data recovery.

Введение

Любая крупная система всегда связана с передачей большого объема информации. Методы и способы хранения информации могут быть различными, однако любой сбой может привести к проблемам, исправление которых займет множество времени, сил и денежных средств. Именно поэтому понимание первопричин таких ситуаций может помочь в их избегании. А в

случае сталкивания с такой проблемой, необходимо знать, какие методы борьбы являются наиболее эффективными и заслуживающими внимания.

Использование вредоносного программного обеспечения

В таблице 1 представлены наиболее популярное вредоносное программное обеспечение, от которого страдают компании и пользователи.

Таблица 1 – Вредоносное программное обеспечение

Название	Метод попадания в систему	Работа внутри системы
Шпионские программы	Могут быть зашиты внутрь скачиваемого файла.	Кража логинов и паролей, запись работы любого ПК в системе, сбор данных о пользователе.
Троянские программы (“троянские кони”)	Вредоносное ПО маскируется под безопасное, из-за чего пользователь самостоятельно заносит его в систему.	После попадания в систему, злоумышленники получают полный доступ, что открывает возможность для провдения любых операций.

Продолжение таблицы 1

Рекламные программы	Неосторожное обращение в сети, открытие подозрительных ссылок.	Позволяют направлять трафик в необходимый браузер, открывать всплывающие окна во время работы.
Черные ходы	Разработчики сами могут оставить доступ к системе без ведома пользователя.	В зависимости от конфигурации в худшем случае может перехватить управление над системой.
Кейлоггеры	Могут быть вшиты в любые программы или установлены случайно.	Запоминают последовательность нажимаемых клавиш, что приводит к утечке данных. Особенно чувствительно в случаях банковских транзакций.
Шифровальщики	Использование программ от неизвестных поставщиков или кибератака с целью	Шифруют данные, что парализует всю систему, включая смежные процессы.

	проникновения.	

Одной из наиболее распространенных причин потерь данных является вредоносное программное обеспечение, которое в свою очередь “заражает” всю систему. Последствия такой ситуации могут быть самыми разными, начиная от потери конкретного файла или группы файлов, заканчивая потерей доступа ко всей системе. Основными методами профилактики таких событий является использование официального лицензированного ПО, а также проверка любых данных, с которыми взаимодействуют пользователи.

Человеческий фактор, отсутствие технического обслуживания или неправильное общение с техникой

Как видно из таблицы номер 1, основным методом попадания в систему вредоносного ПО являются человеческие действия. Иногда пользователь намеренно запускает такой вирус в компьютер, однако в подавляющем большинстве случаев именно неосторожность или незнание об угрозах становятся причиной. То же самое касается случаев, когда удаляются необходимые файлы, форматируются целые разделы с информацией или старые файлы перезаписываются на новые.

Хоть жесткие диски традиционно считаются одними из самых надежных способ хранения данных, даже они могут быть подвержены физическому воздействию, которое приводит к поломкам. В свою очередь, SSD или M2 носители требуют еще более бережного обращения с собой из-за крайней хрупкой архитектуры устройств. Неправильное обращение с техникой может привести даже к большим проблемам, чем системная ошибка, так как физическое восстановление устройства является более тяжелой и кропотливой работой.

Отсутствие технического обслуживания также является распространенной проблемой. Одной из проблем может быть редкая чистка вентиляторов. Это приводит к ухудшению их работы, что в свою очередь сказывается на быстродействии системы, а в некоторых случаях перегрев становится главной причиной поломок. Что касается технической части, то отсутствие проверок системы, хранение избыточного количества файлов и неправильные сохранения также могут привести к замедлению системы или полному ее отключению.

Способы профилактики и исправления ошибок

Несмотря на большое количество причин возникновения проблем, также существуют методы их решения. В случае с человеческим фактором для особо важных операций (удаление, изменение или запись на определенный носитель), должна проводиться полная проверка необходимости этого действия. В некоторых ситуациях должна применяться система с подтверждением от вышестоящего по должности человека или группы лиц.

Техническое обслуживание должно проводиться строго в срок. Это касается как аппаратной, так и технической части. Любая компания должна закладываться в бюджет такую статью расходов, обращаясь к проверенным специалистам. Стоит помнить, что попытка сэкономить на такой важной части, может привести к гораздо более затратным методам восстановления данных.

Однако главным способом минимизировать ущерб в случае нештатной ситуации является наличие работоспособной резервной копии на надежном носителе. Самым эффективным является хранение данных “в облаке”, так как нанести физический вред в таком случае не представляется возможным. Процесс создания резервной копии должен быть неотъемлемой частью работы любого сотрудника, взаимодействующего с данными в рамках информационной системы компании. Именно наличие или отсутствие таких “бэкапов” может предопределить деятельность компании в случае проблемы.

Список литературы

1. Поляков, Я. А. Использование различных подходов резервного копирования баз данных для предотвращения потери данных / Я. А. Поляков, Е. Д. Алехина // Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе : Материалы Всероссийской научно-технической конференции. В 2-х томах, Калуга, 14–16 ноября 2023 года. – Москва: Издательство МГТУ им. Н.Э. Баумана, 2024. – С. 60-62.

2. Фридман, О. Д. Предотвращение риска разрушения и потери ценных данных в банковской сфере / О. Д. Фридман, Д. А. Трунина, Г. О. Чегуров // Научный электронный журнал Меридиан. – 2019. – № 16(34). – С. 42-44.

3. Танкаян, А. И. Информационная безопасность персонального компьютера и современные виды угроз потери данных / А. И. Танкаян, Д. Н. Савинская // Информационное общество: современное состояние и

перспективы развития : Сборник материалов XI международного студенческого форума, Краснодар, 23–27 июля 2018 года. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2018. – С. 114-116.

4. Поляков, А. А. Скрытые риски массовых обновлений данных: как избежать потери и утечки информации / А. А. Поляков // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9, № 12(50). – С. 12-15.

5. Алешин, А. Ю. Эффективные способы борьбы с потерей корпоративных данных / А. Ю. Алешин // Защита информации: IT, правовые и экономические аспекты : Сборник научных трудов Межвузовской студенческой научно-практической конференции, Москва, 16–17 марта 2023 года. – Москва: МИРЭА - Российский технологический университет, 2023. – С. 84-87.

References

1. Polyakov, Ya. A. The use of various database backup approaches to prevent data loss / Ya. A. Polyakov, E. D. Alyokhina // High-tech technologies in instrumentation and mechanical engineering and the development of innovation in higher education institutions : Proceedings of the All-Russian Scientific and Technical Conference. In 2 volumes, Kaluga, November 14-16, 2023. Moscow: Publishing House of Bauman Moscow State Technical University, 2024, pp. 60-62.

2. Friedman, O. D. Preventing the risk of destruction and loss of valuable data in the banking sector / O. D. Friedman, D. A. Trunina, G. O. Chegurov // Scientific electronic journal Meridian. – 2019. – № 16(34). – Pp. 42-44.

3. Tankayan, A. I. Information security of a personal computer and modern types of data loss threats / A. I. Tankayan, D. N. Savinskaya // Information Society: current state and development prospects : Collection of materials of the XI International Student Forum, Krasnodar, July 23-27, 2018. Krasnodar: I.T. Trublin Kuban State Agrarian University, 2018, pp. 114-116.

4. Polyakov, A. A. Hidden risks of massive data updates: how to avoid information loss and leakage / A. A. Polyakov // International Journal of Information Technology and Energy Efficiency. – 2024. – Vol. 9, No. 12(50). – pp. 12-15.

5. Alyoshin, A. Y. Effective ways to combat corporate data loss / A. Y. Alyoshin // Information protection: IT, legal and economic aspects : Proceedings of the Interuniversity Student Scientific and Practical Conference, Moscow, March 16-17 In 2023. – Moscow: MIREA.