



DOI: <https://doi.org/10.15688/NBIT.jvolsu.2024.1.5>

УДК 004.732

ББК 32.971.352

ПРИМЕНЕНИЕ МЕТОДОВ РЕЗЕРВНОГО КОПИРОВАНИЯ ДЛЯ БЕЗОПАСНОСТИ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Олеся Александровна Какорина

Кандидат физико-математических наук, доцент,
заведующая кафедрой информационной безопасности,
Волгоградский государственный университет
davletova.olesya@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Артем Николаевич Юрцев

Магистрант, кафедра информационной безопасности,
Волгоградский государственный университет
IVm-231_595568@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В данной статье рассматривается важность применения методов резервного копирования для обеспечения безопасности систем электронного документооборота. Представлен анализ различных подходов к созданию и хранению резервных копий данных, а также разработаны рекомендации по выбору наиболее эффективных методов. Особое внимание уделено автоматизации процесса создания резервных копий, тестированию процедур восстановления данных и обновлению методов резервного копирования. Описываются основные методы резервного копирования данных: полное резервное копирование, инкрементальное резервное копирование, дифференциальное резервное копирование, обратное инкрементальное резервное копирование, синтетическое резервное копирование. Для выбора наиболее подходящего метода резервного копирования определены параметры, характеризующие эти методы. Проведен анализ методов по выделенным параметрам. В результате исследования делается вывод о том, что правильное применение методов резервного копирования способствует повышению безопасности систем электронного документооборота и снижению рисков потери данных.

Ключевые слова: защита информации, защищенный документооборот, резервное копирование, риски, безопасность.

Система электронного документооборота (далее – СЭД) – это система автоматизации работы с информационными документами на протяжении всего их жизненного цикла,

а также процессов взаимодействия между сотрудниками.

Основной функционал системы электронного документооборота должен включать в

себя следующие возможности работы с документом:

- создание;
- изменение;
- хранение;
- маршрутизация;
- поиск;
- классификация.

Достаточно большое количество систем электронного документооборота предназначены для организации и автоматизации процессов взаимодействия между сотрудниками во время выполнения рабочих задач в рамках определенного бизнес-процесса (передача документов, присвоение заданий отдельным сотрудникам, отправки уведомлений, отслеживания выполнения плана, организация плана выполнения бизнес-цели и т. д.). Документами в системе электронного документооборота могут являться как структурированные объекты, обладающие определенным набором стандартных реквизитов, так и неструктурированные.

Таким образом, системы электронного документооборота обеспечивают: эффективное управление потоками документов в организации; повышение контроля исполнения планируемых работ с определенной в рамках проекта документацией; повышение продуктивности работы сотрудников организации.

В современных условиях развития и организации бизнес-процессов внутри организации внедряемая система электронного документооборота должна решать задачи,

связанные с оптимизацией затрат и экономией ресурсов организации, в том числе и трудовых ресурсов.

В широком смысле информационная безопасность – это совокупность средств защиты информации от случайного или преднамеренного воздействия.

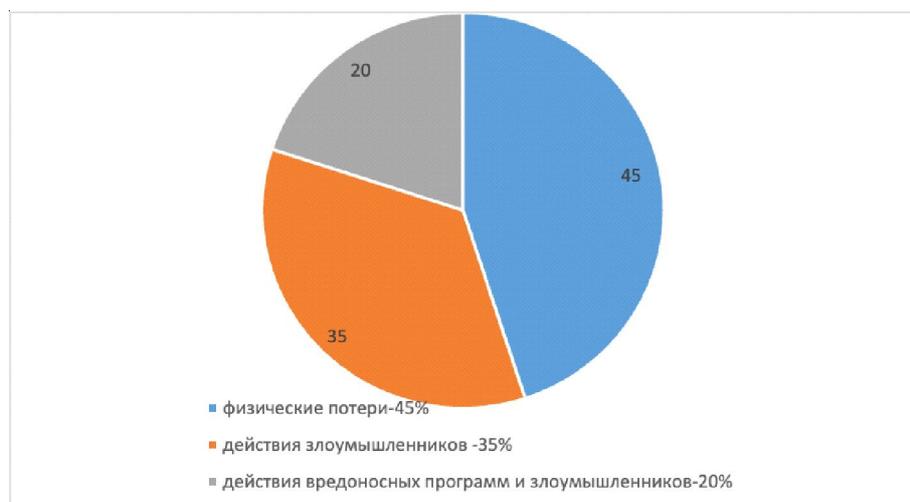
Организованное инсайдерами или киберпреступниками несанкционированное использование, кража или искажение деловой, банковской, коммерческой или статистической информации неизменно приводит к значительным экономическим потерям.

От архитектуры используемого оборудования и специалистов, которые его обслуживают, зависит надежность ИТ-инфраструктуры. Выход сервера или виртуальной машины из строя, поломка жесткого диска приводят к повреждению данных, однако наличие резервных копий поможет быстро восстановить работу компании.

Угрозы для системы ЭДО могут быть внешними и внутренними. Представленная на рисунке статистика показывает, что большая часть потерь информации в системах электронного документооборота приходится на физические потери.

Соответственно, на основании данной статистики, выделим три категории актуальных угроз для систем электронного документооборота:

- 1) физические потери;
- 2) действия вредоносных программ и злоумышленников;



Статистика по потерям информации в системах электронного документооборота

3) ошибки пользователей.

Методы резервного копирования являются одним из основных инструментов для обеспечения безопасности систем электронного документооборота. Резервное копирование (или бэкап – от английского слова «backup») является важным процессом в жизни любой ИТ-структуры.

Для обеспечения безопасности СЭД необходимо:

1. Регулярное создание резервных копий данных: этот метод включает в себя регулярное создание копий всех данных, хранящихся в системе электронного документооборота. Резервные копии могут быть хранены на внешних носителях данных или в облачном хранилище.

2. Использование автоматизированных резервных копий: для упрощения процесса создания резервных копий можно использовать специальные программные средства, которые автоматически создают копии данных с заданной периодичностью.

3. Хранение резервных копий в защищенном месте: важно обеспечить безопасное хранение резервных копий данных, чтобы предотвратить их утрату или несанкционированный доступ.

4. Проведение тестов восстановления: для проверки эффективности процесса восстановления данных из резервных копий необходимо периодически проводить тесты восстановления.

5. Обновление и адаптация методов резервного копирования: системы электронного документооборота могут меняться со временем, поэтому важно периодически обновлять и адаптировать методы резервного копирования для обеспечения их эффективности.

Применение этих методов поможет обеспечить безопасность системы электронного документооборота и минимизировать риски потери данных [1; 2].

Резервное копирование данных можно разделить на несколько типов, каждый из которых отвечает различным потребностям и сценариям.

Создание **полного резервного копирования** означает сохранение всех данных и является наилучшим способом защиты информации, благодаря быстрому и простому вос-

становлению. Однако процесс создания полной копии требует копирования большого объема данных, что делает его трудоемким. Полное резервное копирование является первым шагом для всех других методов резервного копирования.

При использовании **инкрементального резервного копирования** сохраняются только данные, которые были изменены с момента последнего копирования. Этот подход позволяет экономить ресурсы и время, но в случае потери даже небольшой части данных возможны проблемы при восстановлении всего содержимого.

Дифференциальное резервное копирование также экономит ресурсы и время, поскольку оно создает резервную копию только тех данных, которые изменились с момента последнего полного резервного копирования. Для того чтобы восстановить информацию, необходимы всего две копии: полная и последняя дифференциальная резервная копия.

Обратное инкрементальное резервное копирование аналогично другим типам резервного копирования начинается с выполнения полного резервного копирования. После этого создаются инкрементные резервные копии, причем каждая *последующая инкрементная резервная копия* обратима.

Синтетическое резервное копирование начинается с полной резервной копии, за которой следует серия инкрементальных копий. В определенный момент инкрементные резервные копии объединяются с полной резервной копией, синтезируя самую актуальную полную резервную копию [3–5].

Для выбора подходящего вида копирования, необходимо обратить внимание минимум на два параметра – это место для хранения резервной копии и время для выделения на «окно бэкапа».

Для выбора подходящего метода резервного копирования следует учитывать следующие параметры.

Параметр 1. Временной промежуток резервного копирования (большой, средний, малый) – П1.

Параметр 2. Временной промежуток восстановления из резервной копии (большой, средний, малый) – П2.

Параметр 3. Объем памяти для хранения резервных копий (большой, средний, малый) – П3.

Параметр 4. Уровень надежности метода резервного копирования (высокий, низкий) – П4.

Параметр 5. Уровень нагрузки на сеть при выполнении копирования (высокий, низкий) – П5.

Параметр 6. Дублирование информации, что приводит к увеличению времени и объема резервного копирования за счет повторного копирования уже имеющихся данных (высокое, низкое) – П6.

Далее было проведено исследование методов резервного копирования и определены значения параметров, было выявлено, что наиболее подходящими методами резервного копирования данных для обеспечения безопасности систем электронного документооборота является полное, инкрементальное и обратное инкрементальное резервное копирование (см. таблицу).

СПИСОК ЛИТЕРАТУРЫ

1. Бережной, А. Поучительные истории о резервном копировании / А. Бережной // Системный администратор. – 2023. – № 11 (252). – С. 52–57.

2. Дегтярев, Д. И. Безопасная компиляция и архитектуры защищенных модулей / Д. И. Дегтярев, О. А. Какорина // Безопасность информационных систем и технологий в условиях цифровой экономики : материалы IX Всерос. науч.-практ. конф. с междунар. участием, Волгоград, 27–28 окт. 2021 г. – Волгоград : Изд-во ВолГУ, 2021. – С. 23–26.

3. Морозов, М. А. Современные методы резервного копирования данных / М. А. Морозов // XIII Ежегодная научная сессия аспирантов и молодых ученых : материалы межрегион. науч. конф., Вологда, 18–22 нояб. 2019 г. В 2 т. Т. 1. – Вологда : Волог. гос. ун-т, 2019. – С. 175–179.

4. Орлянский, А. А. Обзор методов резервного копирования и восстановления данных и оценка роли носителей информации в операциях резервного копирования / А. А. Орлянский, И. Р. Кольцов, Д. А. Узеньков // Технологии инженерных и информационных систем. – 2023. – № 2. – С. 54–60.

5. Чумбуридзе, Я. А. Основные методы резервного копирования для обеспечения безопасности информации / Я. А. Чумбуридзе // Международный журнал гуманитарных и естественных наук. – 2023. – № 3-2 (78). – С. 57–60. – DOI: 10.24412/2500-1000-2023-3-2-57-60

REFERENCES

1. Berezhnoi A. Pouchitelnye istorii o rezervnom kopirovanii [Instructive Stories About Backup]. *Sistemnyj administrator* [System Administrator], 2023, vol. 11 (252), pp. 52-57.

2. Degtyarev D.I., Kakorina O.A. Bezopasnaja kompiljacija i arhitektury zashhishhennyh modulej [Secure Compilation and Architectures of Protected Modules]. *Bezopasnost informacionnyh sistem i tehnologij v uslovijah cifrovoj ekonomiki: materialy IX Vseros. nauch.-prakt. konf. s mezhdunar. uchastiem, Volgograd, 27–28 okt. 2021 g.* [Security of Information Systems and Technologies in the Digital Economy. Proceedings of the 9th All-Russian Scientific and Practical Conference with International Participation, Volgograd, October 27–28, 2021]. Volgograd, Izd-vo VolGU, 2021, pp. 23-26.

3. Morozov M.A. Sovremennye metody rezervnogo kopirovanija dannyh [Modern Methods of Data Backup]. *XIII Ezhegodnaja nauchnaja sessija aspirantov i molodyh uchenyh: materialy mezhtregion. nauch. konf., Vologda, 18–22 nojab. 2019 g. V 2 t.*

Значение параметров для различных методов резервного копирования

Метод резервного копирования	Параметр					
	П1	П2	П3	П4	П5	П6
Полное резервное копирование	Большой	Малый	Большой	Высокий	Высокий	Высокое
Инкрементальное резервное копирование	Малый	Большой	Малый	Низкий	Низкий	Низкое
Дифференциальное резервное копирование	Средний	Средний	Средний	Высокий	Высокий	Высокое
Обратное инкрементальное резервное копирование	Малый	Малый	Средний	Низкий	Низкий	Низкое
Синтетическое резервное копирование	Малый	Малый	Средний	Низкий	Низкий	Низкое

T. 1 [The 13th Annual Scientific Session of Graduate Students and Young Scientists. Proceedings of the Interregional Scientific Conference. Vologda, Nov. 18–22, 2019. In 2 Vols. Vol. 1]. Vologda, Volog. gos. un-t, 2019, pp. 175-179.

4. Orlyansky A.A., Koltsov I.R., Uzenkov D.A. Obzor metodov rezervnogo kopirovaniya i vosstanovleniya dannyh i ocenka roli nositelej informacii v operacijah rezervnogo kopirovaniya [Review of the Methods of Data Backup and Recovery and Evaluation of the Role of Media in Backup

Operations]. *Tehnologii inzhenernyh i informacionnyh sistem* [Engineering and Information Systems Technologies], 2023, no. 2, pp. 54-60.

5. Chumburidze Ya.A. Osnovnye metody rezervnogo kopirovaniya dlja obespecheniya bezopasnosti informacii [Main Methods of Backup Copying for Information Security]. *Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk* [International Journal of Humanities and Natural Sciences], 2023, no. 3-2 (78), pp. 57-60. DOI: 10.24412/2500-1000-2023-3-2-57-60

APPLICATION OF BACKUP METHODS FOR THE SECURITY OF ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Olesya A. Kakorina

Candidate of Sciences (Physics and Mathematics), Associate Professor,
Head of the Department of Information Security,
Volgograd State University
davletova.olesya@volsu.ru
Pros. Universitetsky 100, 400062 Volgograd, Russian Federation

Artem N. Yurtsev

Master's Student, Department of Information Security,
Volgograd State University
IBm-231_595568@volsu.ru
Pros. Universitetsky 100, 400062 Volgograd, Russian Federation

Abstract. In a broad sense, information security is a set of means of protecting information from accidental or intentional impact. The unauthorized use, theft, or distortion of business, banking, commercial, or statistical information by insiders or cybercriminals invariably results in significant economic losses. The reliability of the IT infrastructure depends on the architecture of the equipment used and the specialists who service it. The failure of a server, virtual machine, or hard drive leads to data damage, but having backup copies will help quickly restore the company's operations. This article discusses the importance of using backup methods to ensure the security of electronic document management systems. An analysis of various approaches to creating and storing backup copies of data is presented, and recommendations for choosing the most effective methods are developed. Particular attention is paid to automating the backup process, testing data recovery procedures, and updating backup methods. The main methods of data backup are described: full backup, incremental backup, differential backup, reverse incremental backup, and synthetic backup. To select the most appropriate backup method, parameters that characterize these methods are defined. The methods were analyzed according to the selected parameters. The study concludes that the correct use of backup methods helps improve the security of electronic document management systems and reduces the risk of data loss.

Key words: information protection, secure document flow, backup, risks, security.