# InfoDiode как инструмент создания «хранилища черного дня»

Сложно представить организацию, в которой информационные системы и обрабатываемые ими данные не стали бы одним из наиболее ценных активов. Информация, хранящаяся на рабочих местах работников и общих файловых ресурсах, базы данных, технологические и финансовые системы, виртуальные машины, конфигурационные файлы программных и аппаратных средств инфраструктуры являются важнейшей составляющей работоспособности любой современной организации. Задача обеспечения сохранности таких активов становится все более значимой. Выход из строя технических средств, ошибки пользователей и администраторов, происшествия техногенного характера – все это может привести к необратимой утрате ключевых активов компании.

Сегодня к этим рискам добавился еще один – атаки злоумышленников. Чем крупнее организация, тем острее стоит данный вопрос. Рост сложности и объема ИТ-инфраструктуры и количества её пользователей увеличивает возможности проникновения и нарушения ее функционирования как со стороны внешнего, так и со стороны внутреннего нарушителя, растет и риск окончательной утраты информации. В последнее время публичных сценариев утраты информации и нарушения работы ИТ-инфраструктуры в результате действий злоумышленников становится даже больше, чем в результате иных, например, техногенных, факторов. Такой риск, очевидно, требует принятия мер, снижающих как вероятность успешного проникновения злоумышленника в инфраструктуру организации, так и вероятность безвозвратной потери ключевых данных.

Для минимизации указанного риска в качестве лучших практик применяется следующий подход к построению СОИБ, состоящий **из пяти функций**, каждая из которых дополняет предыдущие:

1. Организация защиты информации, систем и ресурсов от внешнего влияния (функции – Identify и Protect);
2. Организация сохранности работоспособности систем и доступности информации в случае успешно реализованной атаки на основную инфраструктуру организации (функции – Detect и Respond);
3. Обеспечение возможности восстановления информационных систем и данных, ресурсов и услуг, пострадавших в результате инцидента безопасности (функция – Recover).

В указанном подходе возможность корректно и оперативно восстановить данные и системы после их компрометации или утраты в основной инфраструктуре – одна из ключевых задач систем резервного копирования и специализированных узлов хранения. Организация их защиты требует комплексного подхода.

AMT GROUP

Тел: +7 (777) 2142677 Email: info@infodiode.kz

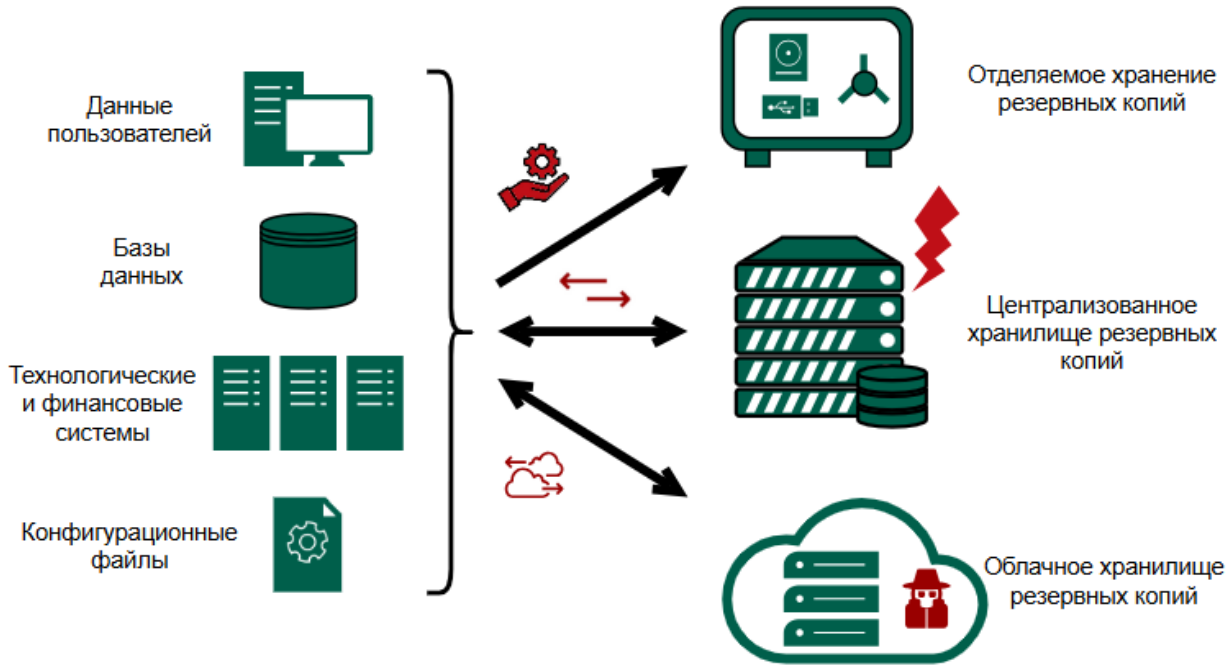
www.infodiode.kz

www.amt-group.kz

## Подходы к организации защиты систем резервного копирования

Исходя из места размещения резервных копий критичных данных можно выделить три основных подхода к организации защиты систем резервного копирования:

1. **Отделяемое хранение резервных копий**. Такой подход подразумевает ручной или автоматизированный механизм, осуществляющий запись информации на съемный носитель, на котором эти данные хранятся отдельно от инфраструктуры организации, либо ручной перенос данных с использованием этого носителя в физически изолированное хранилище. Ключевыми вопросами обеспечения безопасности для такого подхода являются обеспечение физической безопасности съемных носителей, а также защита от внутреннего нарушителя.
2. **Централизованное хранилище резервных копий.** Другой опцией является построение единого централизованного хранилища резервных копий внутри инфраструктуры организации. В такое хранилище можно построить канал передачи данных и сделать процесс резервного копирования полностью автоматическим. При этом данный подход является требовательным к средствам обеспечения защиты как самого хранилища, так и канала передачи.
3. **Облачное хранилище резервных копий.** Для реализации последней цифры правила «3-2-1» современные провайдеры облачных услуг предлагают использование публичного облака в качестве хранилища резервных копий. Данный подход позволяет строить георасределенные хранилища и в том числе снижать риск утери данных и при реализации техногенных угроз. Основной проблемой при использовании такого подхода является то факт, что инфраструктуру провайдера невозможно оценить с точки зрения её защищенности от внешнего и внутреннего злоумышленника, и фактически это перенос риска, а не его минимизация.




Любой подход с построением централизованного хранилища резервных копий требует тщательной проработки вопросов обеспечения безопасности хранилища и соблюдения регламентов резервного копирования. Это связано с тем, что в случае компрометации инфраструктуры организации наличие постоянного канала связи с хранилищем резервных копий может позволить злоумышленнику уничтожить, зашифровать или скомпрометировать все его содержимое. Такое развитие событий может стать «точкой невозврата» для организации.

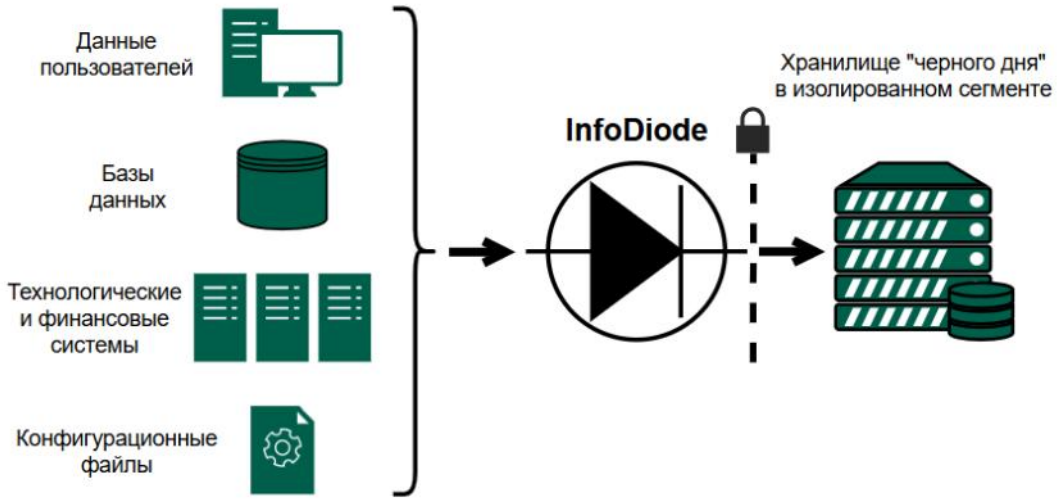
## Направления мероприятий по защите хранилища резервных копий

Защита хранилища резервных копий может строиться по двум основным взаимодополняющим направлениям:

1. **Применение встроенных и наложенных СЗИ, основная функция которых базируется на программной компоненте (программного обеспечения):** механизмы проверки контента для ограничения записи нелегитимных файлов, антивирусные средства, «песочницы» для борьбы с заражением вирусами, межсетевые экраны и средства аутентификации и авторизации для защиты от несанкционированного воздействия, средства шифрования хранилища и канала для обеспечения конфиденциальности и целостности содержимого, write once хранилища.
2. **Построение хранилища резервных копий, максимально отделенного от основной инфраструктуры, с использованием аппаратных средств и имеющего строго ограниченный канал передачи резервных копий.** В ряде случаев такие хранилища получают название «хранилища черного дня», предполагая, что они используются как последний доступный инструмент восстановления данных.

## Применение устройств класса «диод» для создания «хранилища чёрного дня»

В условиях активных атак на ИТ-инфраструктуру наиболее корректным с точки зрения локализации рисков ИБ для защищенных хранилищ резервных копий является совместное применение СЗИ, обеспечивающих функцию безопасности за счет программных решений, и программно-аппаратных СЗИ, функция безопасности которых обеспечивается физическим устройством. Второй тип устройств получил название - «диоды данных». «Диод данных» создает однонаправленный канал в «хранилище черного дня». Такой канал позволяет обеспечить непрерывную, надежную и безопасную загрузку резервных копий в изолированный сегмент, доступ к которому строго ограничен, а вектор атаки серьезно локализован. Технология однонаправленной передачи данных, основанная на принципах физической изоляции более доверенного сегмента от менее доверенных, обеспечивает возможность передачи информации в одном направлении и нивелирует риски эксплуатации злоумышленником двунаправленного канала для организации атаки. За счет таких функций безопасности злоумышленники фактически атакуют «черный ящик»: не имеют возможности определить, какие объекты находятся за границей сегмента, как обрабатываются входящий и исходящий потоки, какие СЗИ используются для защиты этих потоков, не получают реакцию систем на попытки деструктивного воздействия, не знают, зафиксировано ли их деструктивное воздействие на защищаемый сегмент. Такие возможности многократно повышают сложность, длительность, стоимость атак на «хранилище черного дня» и добавляют специалистам ИБ время для обнаружения и купирования атаки, и, в целом, делают атаку нерентабельной.




AMT GROUP
Тел: +7 (777) 2142677 Email: info@infodiode.kz
www.infodiode.kz
www.amt-group.kz

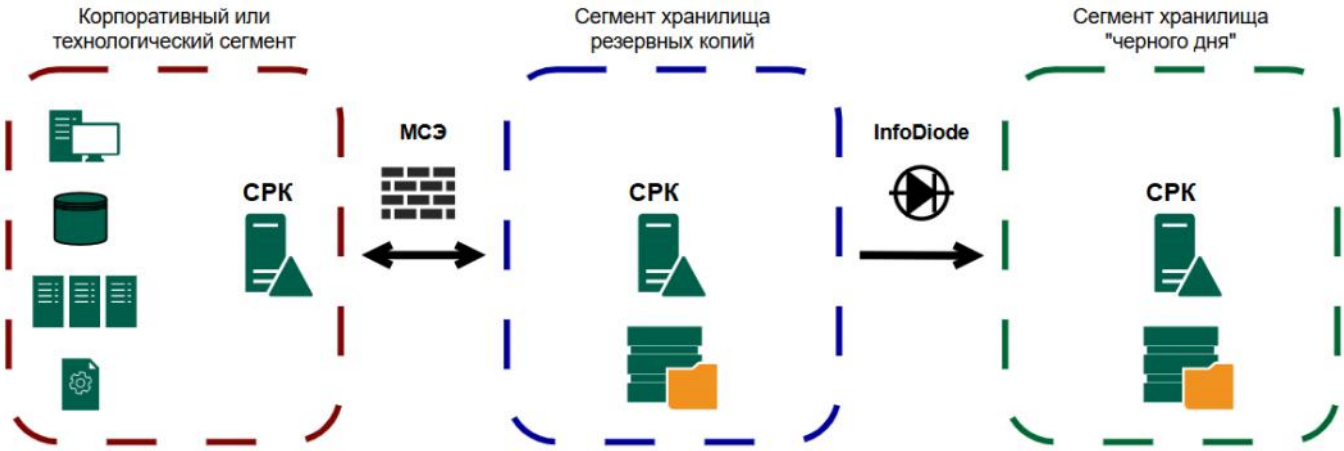
## Сравнение различных подходов для создания хранилища резервных копий

Следует отметить, что, будучи использованным только автономно, каждый из указанных подходов к построению хранилища резервных копий имеет свои достоинства и недостатки, которые необходимо учитывать при его проектировании с учетом МУиН и реальных возможностей ИТ-инфраструктуры организации.

| Направление | Плюсы | Минусы |
|---|---|---|
| **Отделяемое хранение резервных копий** | Физически изолированный процесс переноса данных и физически изолированный от основной ИТ- инфраструктуры организации сегмент хранения резервных копий. Сложность компрометации при условии использования дополнительных инструментов контроля и переноса («песочницы», антивирусы и т.п.) | Неудовлетворительная скорость выполнения операций, ограничения на каналы передачи данных. Необходимость в дополнительном персонале (трудозатраты). В ряде случаев (требуемая скорость, объемы) невозможность применения такой схемы резервного копирования. Сохраняющаяся потребность в дополнительных программных решениях и СЗИ, риски компрометации носителей. |
| **Централизованное хранилище резервных копий с применением только СЗИ, функции безопасности которых сосредоточены в программном обеспечении** | Полная сетевая связность между сетевыми сегментами-источниками резервных копий и сегментами-приемниками. Более высокие скорости резервного копирования. Возможность онлайн контроля статуса и состояния резервных копий. | Программные решения имеют уязвимости, в том числе «уязвимости нулевого дня», могут быть некорректно сконфигурированы. Существует высокая вероятность компрометации и утери резервных копий, особенно в случае действий высококвалифицированных злоумышленников. Решения не позволяют построить полноценное «хранилище черного дня» за счет применения для защиты хранилища только программных решений. |
| **Централизованное хранилище резервных копий с применением только аппаратных или аппаратно-программных решений класса «диод» (InfoDiode) – «хранилище черного дня», функция безопасности которых обеспечивается физическим устройством** | Максимально изолированный от основной ИТ-инфраструктуры организации сегмент хранения резервных копий. Физическая однонаправленность передачи данных внутрь «хранилища черного дня», разрыв двунаправленного сетевого соединения, «разрыв протоколов» гарантируют невозможность удаленного воздействия на инфраструктуру хранилища, исключают ransomware атаки, делают стоимость атаки и ее сложность непривлекательной для злоумышленника. Сохраняется возможность автоматической передачи резервных копий и автоматизация практически всех традиционных процессов резервного копирования. | Невозможность удаленного контроля за резервными копиями - только при локальном или временном сетевом доступе (например, с использованием устройство класса «инфо реле» - InfoRelay). Более низкие скорости резервного копирования за счет применение средств однонаправленной передачи данных. Дополнительные затраты на процесс периодического контроля целостности резервных копий (организационные и программные меры). |
| **Облачное хранилище резервных копий** | Перенос ответственности (в том числе юридически) за построение хранилища резервных копий и за обеспечение его защищённости на провайдера облачных услуг. Географическая отделенность информационных систем и данных от резервного хранилища. | Невозможность контроля за инфраструктурой провайдера как в части её защищенности от атак злоумышленников, так и в части контроля доступа сторонних лиц к критичным данных организации. Законодательный запрет передачи определенных видов данных третьим лицам (банковская тайна, врачебная тайна и т.д.). |

## Применение InfoDiode для создания «хранилища чёрного дня»

Анализ таблицы сравнения решений показывает, что построение надежного и защищенного от внешних угроз хранилища «черного дня» может быть выполнено только за счет применения комплекса решений. В частности, в качестве «транспорта» могут применяться решения по физически однонаправленной передаче данных класса «диоды данных», например, InfoDiode, в то время как усиление защиты хранилища выполняется с использованием дополнительных программных средств защиты. В зависимости от конкретной Модели Угроз и Нарушителя (МУиН) дополнительными инструментами могут быть: механизмы контроля целостности, антивирусные средства, средства аутентификации и авторизации, средства шифрования, встроенные функции безопасности самой системы резервного




Стоит отметить, что использование хранилища «черного дня» не требует перестроения текущих процессов создания и хранения резервных копий. Хранилище «черного дня» может быть развернуто как **«последний рубеж обороны»** для хранения наиболее значимых резервных копий путем интеграции с текущими системами резервного копирования. Единственным требованием выступает необходимость выделения такого хранилища **в отдельный сетевой сегмент**.

Примером такого комплексного подхода к построению хранилища «черного дня» является совместная интеграция решений компаний Киберпротект и АМТ-ГРУП. В его основе лежит применение системы резервного копирования Кибер Бэкап в части настройки плана резервного копирования и плана репликации резервных копий и системы однонаправленной передачи InfoDiode в части обеспечения «однонаправленного транспорта» бэкапов в изолированное хранилище «черного дня». Это решение дает все необходимые средства для организации непрерывного процесса резервного копирования, обеспечивая высокий уровень защищенности даже в случае компрометации основной инфраструктуры организации.