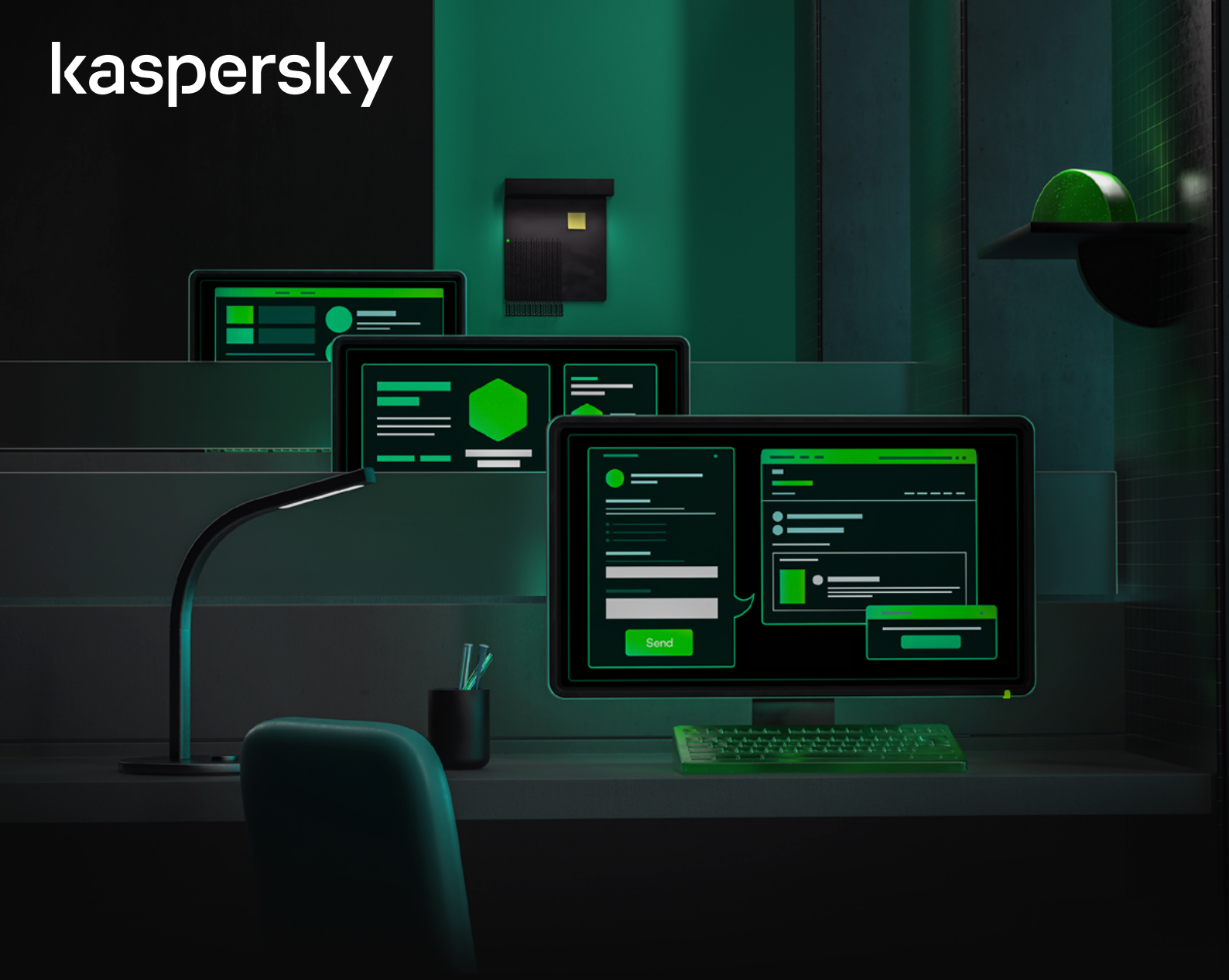
kaspersky




# Рекомендации при инциденте ИБ: взлом IT-инфраструктуры с шифрованием или удалением данных

# Содержание

## О чём пойдёт речь

Первоочередные действия, если вашу IT-инфраструктуру взломали/зашифровали/удалили. К кому обращаться за помощью, в чём эта помощь может заключаться и как получить её эффективно. Что делать после инцидента? Что делать, если есть подозрение на взлом, но нет уверенности? Как пошагово проходит реагирование на такой инцидент? Как подготовиться к реагированию, чтобы быстрее восстановить работу компании и сократить риски уничтожения IT-инфраструктуры и самой компании?

**Настоящие рекомендации предназначены в первую очередь для команд IT и ИБ СМБ (SMB)** и разработаны в целях быстрого и эффективного реагирования на инцидент с привлечением внешней экспертной организации и не адресованы экспертам DFIR (Digital Forensic and Incident Response) или SOC (Security Operations Center) крупных и крупнейших компаний, т. к. предполагается, что такие эксперты — профессионалы в своём деле — и руководствуются в своей работе промышленными тематическими рекомендациями и стандартами. Настоящие рекомендации предназначены для подготовки и принятия мер минимизации сроков восстановления (и сокращения убытков пострадавшей компании) и не содержат детальных рекомендаций по снижению вероятности (предотвращению) самих инцидентов, т. к. существует большое количество материалов, стандартов и консультационных услуг в этой части.

## Цели. Зачем разработаны эти рекомендации и в чём их польза?

Обычно при шифровании IT-инфраструктуры главная и понятная цель — как можно скорее вернуть компанию к нормальной работе. Но есть и другие, не менее важные: выдворить злоумышленника из инфраструктуры, выяснить способ его проникновения в инфраструктуру и предотвратить повторное проникновение, выявить все последствия его деятельности, минимизировать ущерб клиентам и контрагентам, репутации, штрафные санкции и т. д.

Самая распространённая ошибка в такой ситуации — это сосредоточиться только на главной цели по восстановлению систем и данных, забыв о том, что пока злоумышленник не изгнан, не обрублены все его средства доступа и пути возвращения в вашу инфраструктуру, он в любой момент может снова всё удалить или зашифровать. То есть выполнение каких-либо работ по восстановлению или смене паролей совершенно бессмысленно без предварительного устранения доступа злоумышленника к инфраструктуре.

Таким образом, если в случае обычного системного сбоя определено и проверено время восстановления IT-инфраструктуры и данных, которое может составлять десятки минут или несколько часов, то в случае её разрушения злоумышленниками время восстановления может составить несколько дней или недель и будет складываться из следующего: потраченное на безрезультативные действия время + время на принятие решения о реагировании + время на реагирование на инцидент + время восстановления IT-инфраструктуры и данных. При этом важно понимать, что в процессе реагирования на инцидент вся или часть вашей инфраструктуры будет всё ещё недоступна для работы.

**Цель настоящих рекомендаций — исключить трату времени на нецелевые действия и минимизировать расход времени на принятие решения о реагировании и на само реагирование с тем, чтобы минимизировать совокупное время на восстановление**. В общем случае применение настоящих рекомендаций может сократить срок восстановления возможности работы компании с 10 – 15 дней до 5 – 7 дней.

## Почему проблема не может быть решена только силами IT и почему нужно готовиться заранее?

Атаки, проводимые злоумышленниками на корпоративный сектор с использованием программ вымогателей (шифровальщиков) для уничтожения данных или кражи конфиденциальной информации, в большинстве случаев являются полностью человекоуправляемыми! Утверждение «Мы поймали шифровальщика!» зачастую неверно. Таким образом, речь идёт не о разовой человеческой ошибке и не о техническом сбое (который может повторяться), а о целенаправленном вредительском воздействии на все или любые элементы вашей инфраструктуры и на ваших сотрудников, в любое время и адаптивно, с учётом ваших ответных действий. То есть речь идёт о киберборьбе.

Шифрование или удаление данных, а также проведение несанкционированных платежей в ДБО злоумышленники часто инициируют ночью, в пятницу или в выходные, перед праздниками или во время праздников, чтобы у вредоносной программы было больше времени на работу, а у компании – меньше времени на реагирование (сотрудники ушли на выходные и могут быть недоступны). Именно поэтому рекомендуем всегда действовать быстро и без оглядки на день недели или время суток. Для этого необходимо проработать как минимум три компонента:

1. Понимание того, **что нужно делать** и в какой последовательности (или параллельно). Неэффективные действия продлевают простой в работе компании и помогают злоумышленникам.
2. Наличие **доступных в такой ситуации ресурсов**: работники, резервные мощности, резервные копии данных и ПО, финансы, профессиональные внешние эксперты. Если у вас не осталось резервных копий, все деньги украдены злоумышленниками, персонал недоступен и вы не знаете, к кому обратиться за помощью – о быстром восстановлении работы говорить сложно.
3. Готовность действовать: **решение и воля уполномоченного лица, отрепетированные действия**. Без решения и поддержки руководства компании технический персонал не будет действовать полно и правильно, а без репетиции – будет действовать нерешительно и нескоординированно.

Данные рекомендации направлены на проработку всех этих трёх компонентов.

## Что можно сделать заранее?

### Генеральный директор/ CEO/акционер

Коротко:

- Довести данные рекомендации до ответственных за IT и ИБ.
- Проверить, что все всё могут и у всех всё есть, что все подготовительные шаги выполнены.
- Провести «штабные учения»: кто, что и в каком порядке делает и сколько у него это занимает времени. **Важно, чтобы ответственный за ИБ в компании вёл данные учения и имитировал устно действия злоумышленников, а также недоступность ресурсов компании.**
- Оценить время простоя в работе компании при ИБ-инциденте с шифрованием всей инфраструктуры.
- При инциденте привлечь все возможные ресурсы и действовать решительно.
- Поддерживать работников в ходе ликвидации последствий инцидента, а не наказывать!

### Ответственные за ИБ (CISO) и за IT (CTO/CIO)

Коротко:

- Разработать план реагирования в случае успешной кибератаки (с самыми печальными последствиями).
- Предусмотреть резерв оборудования, финансов и т. д.
- Уделить особое внимание безопасности бэкапов данных и самого ПО («3-2-1»).
- Защитить саму систему резервного копирования и предусмотреть внесистемное хранение паролей, сетевой схемы, иного необходимого в случае уничтожения инфраструктуры.
- Провести учения по реагированию и измерить время и стоимость простоя.
- Выбрать партнёров для DFIR и заключить с ними NDA + рамочный договор или подписку на услуги.
- В случае подозрений на взлом – проводить Compromise Assessment.

## Может, просто заплатить выкуп? Не рекомендуем, но решать вам

Вопрос оплаты выкупа злоумышленникам в данном методическом материале подробно не рассматривается и в общем случае не рекомендуется, так как:

1. Нет гарантий расшифрования данных злоумышленниками после получения выкупа.
2. В ряде случаев злоумышленники, даже получив выкуп, сознательно не будут расшифровывать данные компании из РФ по принципиальным соображениям.
3. После оплаты выкупа за расшифровку вас могут попросить о втором выкупе для удаления похищенных у вас данных.
4. Вас могут зашифровать повторно после оплаты выкупа якобы «другие» злоумышленники и также потребовать выкуп.
5. Нет гарантий, что предоставленные злоумышленниками средства расшифрования в принципе будут работать корректно для всех ваших данных.
6. Ваш банк может отказаться провести соответствующую транзакцию по соображениям ПОД/ФТ.
7. После оплаты выкупа **к вам могут быть предъявлены претензии на предмет финансирования терроризма** по результатам анализа платежей государственными органами.
8. Вам, в конце концов, следует самостоятельно принять это решение с учётом всех рисков и последствий.

Если вы всё же решили пойти на поводу у злоумышленников и заплатить выкуп, рекомендуем обратиться за помощью в проведении переговоров к тем компаниям, которые имеют экспертизу в проведении DFIR и речь о которых пойдёт ниже.

## Как это вообще могло произойти?

Первоначальный доступ к вашей инфраструктуре мог быть получен, например, следующими способами:

- VPN, RDP, SSH, OWA/Exchange, Jira, Confluence, Gitlab, Sharepoint и т. д. – неисправленная уязвимость или подбор пароля (слабые или утекшие пароли, стандартный пароль вендора, типовой пароль сотрудника или организации, неконтролируемый вами перебор пароля внешним злоумышленником).
- Фишинг, в том числе с доверенных адресов коллег и контрагентов после взлома их учётных записей и/или компаний.
- WEB-приложение – уязвимость (например, год или несколько месяцев не патченный Bitrix или установленный к нему и забытый всеми модуль, на который обновления устанавливаются отдельно от центрального модуля, о чём знают не все администраторы), дефолтные пароли или доступные из интернета служебные интерфейсы.
- Кибератаки, проводимые за счёт компрометации доверительных отношений между организациями. Так, например, злоумышленники могут скомпрометировать менее защищённого партнёра (подрядчика, поставщика и т. п.) и от его имени (учётной записи) получить доступ к ресурсам целевой инфраструктуры.
- Атаки на цепочку поставок – кибератаки, при которых злоумышленники компрометируют продукты поставщиков программного или аппаратного обеспечения, чтобы атаковать конечных пользователей их продуктов.
- Внутренний нарушитель – сознательный вредитель или несознательный нарушитель требований безопасности (в том числе подкупленный или шантажируемый злоумышленниками). Если сотрудник, обманутый мошенниками, передаёт им всё своё имущество, берёт в их интересах кредит – что мешает злоумышленникам попросить его в дополнение к сделанному сообщить его пароль и код для двухфакторной аутентификации либо установить программу удалённого управления на его домашний или рабочий компьютер?
- И так далее...

# Первоочередные рекомендации

Что рекомендуем делать в первую очередь, если у вас нет заранее разработанного и проверенного DRP плана (**лучше всего выполнять указанные ниже работы по возможности параллельно**):

1. **Заблокировать доступ к ДБО в банках**. Первым делом целесообразно обратиться в ваш банк для блокировки и осуществить сверку последних платежей для поиска несанкционированных операций. Используйте средства связи вне вашей скомпрометированной инфраструктуры.
2. **Изолировать, но не выключать и не перезагружать заражённые узлы**. Не отключать электропитание хостов, ПК, виртуалок, но отключать их от вычислительной сети (ЛВС) – проводной и беспроводной (Wi-Fi), отключить SAN сеть данных во избежание шифрования данных на СХД. Прекратить работу на таких узлах. В отдельных случаях в энергозависимой памяти могут сохраниться важные улики или даже ключи шифрования для зашифрованных злоумышленниками файлов.
3. **Изолировать ценное: срочно отключить от ЛВС серверы с резервными копиями и важными данными** (контроллеры доменов, гипервизоры, серверы БД, файловые серверы, системы централизованного управления (в т. ч. антивирусным ПО) и т. п.). Лучше – физически вынуть Ethernet-кабель. Сделать дополнительные «снапшоты» текущего состояния для них, если они находятся в виртуальной среде. Рассмотреть сетевую изоляцию сегментов сети и/или отключение вашей сети от сети интернет. Возможно, злоумышленники ещё не успели до них добраться или до конца зашифровать.
4. **Выгрузить списки паролей и записи DNS-сервера** на съёмный носитель и на бумагу. Без доступа к узлам и серверам, а также без их адресов дальнейшие работы по восстановлению будут крайне затруднены.
5. **Не подключать накопители информации с важной информацией, включая резервные копии, к потенциально скомпрометированным системам** до момента установления источника угрозы данным (вредоносного ПО, которое может повредить данные на таких носителях). При подключении внешних жёстких дисков или лент с резервными копиями следует обращаться с ними максимально бережно, так как есть риск, что подключение носителя информации к потенциально скомпрометированной системе приведёт к утрате данных. В крайнем случае сделайте на изолированном безопасном компьютере копию носителя перед его подключением и не подключайте все носители одновременно. Если у вас есть резервные копии в удалённой инфраструктуре (например, вы арендовали IaaS и разместили в нём резервные копии) – предупредите оператора этой инфраструктуры/сервиса об инциденте в целях повышения его бдительности и сохранности таких бэкапов. Подключайте носители резервных копий в режиме «только чтение» в случае, если блокировка записи осуществляется технически отдельным нескомпрометированным средством или на стороне самих носителей, но не системы резервного копирования или той системы, к которой осуществляется подключение носителя.
6. **Не переустанавливать операционные системы пострадавших систем до момента сбора с них данных с криминалистически значимой информацией**. В ряде случаев переустановка той или иной системы может негативно сказаться на процессе реагирования и не позволить выявить источник первоначальной компрометации. Перед переустановкой ОС обязательно собирайте триажи (слепок данных с криминалистически значимой информацией), побитовые образы дисков, поврежденные файлы дисков виртуальных машин и т. д.
7. **Проверить исходящий в сторону сети интернет сетевой трафик и рассмотреть целесообразность изоляции от сети интернет всей или части вашей сети**. Возможно, злоумышленники ещё скачивают какую-то конфиденциальную информацию, и вы можете успеть разорвать соответствующие сетевые сессии. При необходимости – отключите от сети интернет вашу инфраструктуру или изолируйте на уровне сетевого взаимодействия поражённые сетевые сегменты. Если вы обнаружили признаки нелегитимного исходящего сетевого трафика, то фиксируйте их с помощью скриншотов или делая выгрузки журналов (логов) сетевого оборудования/средств контроля за трафиком. Данные сведения могут быть полезны для последующего расследования кибератаки и реагирования на неё.
8. **Позаботиться о режиме работы персонала**, задействованного с вашей стороны, в разрешении проблем в условиях инцидента: специалистов по цифровой криминалистике и реагированию на инциденты, специалистов, которые будут заниматься восстановлением IT-инфраструктуры и данных, специалистов по взаимодействию с правоохранительными и надзорными органами, по взаимодействию со СМИ и партнёрами, а также о режиме работы остальных сотрудников. **Определить координатора (РП) и принимающее решения лицо** (лучше, если это будут разные люди), обеспечить связь и их доступность для участников работ. **Крайне важно, чтобы все коммуникации были ВНЕ поражённой инфраструктуры**, т. к. корпоративную переписку, а также чаты мессенджеров, чьи сессии были авторизованы на устройствах скомпрометированной инфраструктуры, могут читать злоумышленники. Как правило, в ситуациях расследования взлома и восстановления инфраструктуры рекомендуется использовать личные устройства и установленные на них мессенджеры вроде MAX, eXpress или Telegram, убедившись, что отключены неизвестные сессии и в соответствующие аккаунты сотрудники не входили на корпоративных устройствах.

9. **Во избежание компрометации последующих коммуникаций и их прочтения злоумышленниками** завершить все сессии мессенджеров (MAX, eXpress, Telegram и иные), авторизованные в атакованной инфраструктуре, с применением нескомпрометированных персональных мобильных устройств.
10. **Решить, какие у компании цели при реагировании на инцидент**: правда ли будем стараться доводить до суда и огласки? Или наоборот – будем стараться не допустить «хайпа»? Достижение каждой из целей стоит затрат, а цели могут друг другу противоречить.
11. **Обратиться за консультацией в компании, которые оказывают услуги по реагированию на инциденты**. Специалисты данных компаний могут запросить некоторые детали по кибератаке и, если представляется возможным, предоставить какую-либо полезную информацию об атаке. Например, об известных способах закрепления данных, атакующих в инфраструктурах, об их мотивации, о той или иной вредоносной программе и т. д. Помимо этого, у данных компаний можно запросить инструменты и инструкции для сбора информации, необходимой для реагирования и расследования инцидента. В ряде случаев вам могут помочь определить вид шифровальщика и дать рекомендации по восстановлению хотя бы части зашифрованных данных.
12. **Провести реагирование на инцидент** (DFIR, Digital Forensic and Incident Response / цифровая криминалистика и реагирование на инциденты) своими силами или, при отсутствии должных компетенций, обратиться в профильные компании, занимающиеся этим на повседневной основе.

Такую услугу оказывает «Лаборатория Касперского». Сервис Kaspersky Incident Response включает полный цикл расследования инцидентов и реагирования на них – от сбора доказательств и раннего реагирования на инцидент до выявления дополнительных следов взлома и подготовки рекомендаций по устранению заражения и ликвидации его последствий.

Перед началом восстановления необходимо локализовать инцидент, лишить атакующих возможности взаимодействовать со скомпрометированной инфраструктурой, а также минимизировать ущерб от их действий. Реагирование на инцидент позволит выявить причины его наступления, снизит риски повторного наступления негативных событий и обеспечит возможность безопасного восстановления работоспособности IT-инфраструктуры и её отдельных систем. **Помните, что антивирусные продукты не способны в полной мере помочь вам в выявлении средств закрепления злоумышленников, т. к. для этого довольно часто используются свободно распространяемые программы, не детектируемые традиционными защитными средствами**.

13. **Сохранять копии выявленного вредоносного ПО**, подозрительных исполняемых файлов для их изучения командой DFIR.
14. **Не загружать на популярные ресурсы (например, virustotal.com и др.) неизученные (неизвестные) образцы вредоносных программ** (даже известных семейств, например, Lockbit) для проверки антивирусными модулями. Таким образом вы можете раскрыть информацию и характер атаки на вас. Нередки случаи, когда злоумышленники в экземпляры вредоносного ПО добавляют домены, учётные записи и иные сведения о жертве. Доверьте анализ выявленного ВПО команде DFIR, которая изучит его, даст рекомендации в отношении него и подготовит отчёт, в т. ч. по функциональному предназначению ВПО.
15. **Обратиться в правоохранительные органы** (после согласования с юристом / юридической службой вашей организации).
16. **Оценить необходимость привлечения разных подрядчиков: отдельно на реагирование и отдельно на восстановление IT-инфраструктуры**. У разных подрядчиков могут быть разные компетенции в ИБ и в IT, а также различные ресурсы и расценки на услуги.
17. **Рассмотреть возможность проинформировать клиентов и партнёров об инциденте**. Ваша IT-инфраструктура может быть использована для атаки на партнёров: могут быть скомпрометированы учётные записи от их систем, может быть осуществлена атака на партнёра через установленный с вашей инфраструктурой VPN, атака на размещённую в вашей IT-инфраструктуре физическую или виртуальную инфраструктуру / информацию иных обществ и так далее. Все тексты сообщений, направляемых в связи с инцидентом вашим партнёрам, клиентам, иным третьим лицам рекомендуется предварительно согласовать с юридической службой / юристом вашей организации.

18. **Определить одно лицо, ответственное за коммуникации**. Как правило, это человек из службы PR/маркетинга. Хорошо, если есть уже подготовленные и согласованные с юридической службой / юристом вашей организации черновики заявлений для клиентов и СМИ на случаи:
    - продолжительной недоступности сервисов,
    - размещения на сайте вашей компании противоправной информации,
    - утечки информации (и ПДн) из вашей компании.

    Необходимо понимать, что все публичные коммуникации будут изучать злоумышленники, и в случае подготовки текстов в пределах поражённой инфраструктуры злоумышленники также будут читать готовящиеся материалы. Поэтому рекомендуем все материалы готовить вне вашей инфраструктуры и осуществлять внешние коммуникации только по мере необходимости и после обсуждения с ответственным за обеспечение ИБ в вашей компании.

19. Следует также **подумать о коммуникации с сотрудниками**, так как многие из них в нестандартной ситуации могут быть напуганы и не знать, что делать, либо делать что-то, что помешает работе или DFIR. В первую очередь необходимо успокоить сотрудников и сообщить им, что проблема временная, компания вернётся к нормальной работе, за невыполнение KPI никто не будет наказан. Затем объясните сотрудникам, что можно и что нельзя говорить родственникам/друзьям/знакомым или писать в социальных сетях и почему, а также какую часть деятельности можно выполнять альтернативными путями, что можно и нужно говорить клиентам и партнёрам.
20. **Повесить на сайт заглушку – хотя бы о «техническом сбое»**. Лучше всего, если это будет заглушка со ссылкой на социальную сеть, в которой компания ведёт свой блог. Так вы сможете оперативно информировать клиентов и контрагентов о ситуации с использованием внешнего ресурса, не отвлекая на это задействованный в DFIR и восстановлении IT-инфраструктуры персонал.
21. **Делом и словом поддержать сотрудников, которые задействованы в ликвидации инцидента**. Следует воздержаться от поспешных кадровых решений, негативных эмоций и выяснения того, кто виноват – как минимум до завершения DFIR и полного восстановления IT-инфраструктуры и данных. Вы в любом случае понесёте финансовые расходы и убытки — но не лучше ли понести расходы на премирование исправляющих ситуацию сотрудников, чем понести убытки от простоя на ту же или гораздо большую сумму в случае их бездействия или увольнения? **Помните, что демотивированный сотрудник меньше всего будет заинтересован в реагировании на инцидент, а сотрудник, который допустил (по своей вине или нет), но исправил ситуацию, для вашей компании лучше и ценнее нового**.

# Что такое DFIR, и как за ним обращаться?

DF (Digital Forensics) – это извлечение дисков (или снятие их копий) либо снятие дампа памяти включенного компьютера и передача таких дисков/копий/дампов или подозрительных файлов на анализ цифровым криминалистам для исследования и поиска следов действий злоумышленников, а также восстановления удалённых файлов.

IR (Incident Response) – это выявление способа компрометации, закладок, фактов утечки данных и реагирование на выявленное в целях минимизации негативных последствий, восстановления работоспособности IT-инфраструктуры и принятие мер по недопущению повторения инцидента.

Ряд компаний на российском рынке предлагают услуги DFIR и CA как в режиме экстренного обращения (DFIR), так и в плановом (CA). Так, например, АО «Лаборатория Касперского» оказывает как сервис по экстренному реагированию на инциденты и ликвидации последствий нарушения системы безопасности (Kaspersky Incident Response), так и сервис оценки компрометации (Kaspersky Compromise Assessment).

С коммерческими компаниями возможно заключение договора заранее, например, в виде рамочного договора или предварительно оплаченной подписки на услугу. Целесообразно удостовериться в наличии у компании необходимых ресурсов, инструментов, квалификации, разрешений. Так, субъекты КИИ обязаны взаимодействовать с НКЦКИ в установленном законом и подзаконными актами порядке и, в частности, информировать НКЦКИ об инцидентах, в первую очередь, напрямую или через аккредитованные центры (заключившие соглашение на переходный период), перечень которых опубликован на сайте ГосСОПКА.

Настоящие рекомендации не отражают специфику КИИ и предназначены для наиболее общего случая.

## С какой информацией обращаться в экспертную компанию за DFIR?

Как правило, требуется предоставить:

- В связи с чем обращаетесь (краткое описание проблемы).
- Размер компании (в количестве сетевых узлов/хостов и/или сотрудников).
- Контакты для связи с вами (телефон, почта).
- Дополнительную информацию, например: наименование компании и её месторасположение.

Как правило, в течение не более чем 24 часов (но обычно – довольно быстро, спустя минуты) с вами связывается дежурный сотрудник компании для уточнения деталей и предлагает проведение DFIR в режиме офлайн (с выездом) или онлайн (удалённо), а также уточняет дополнительные организационные и технические детали.

В случае выезда (проведение DFIR офлайн) от вас требуется: определить дату и время выезда, назвать адрес выезда, предоставить ФИО и контакты (телефон) ответственного за встречу на месте, заказать пропуска, при необходимости также обеспечить парковку.

Что не стоит делать: назвав дату и время выезда, отменять выезд, т. к. сразу после вашего подтверждения оперативная группа подрядчика начинает подготовку к выезду, в том числе отменяет запланированные сотрудниками встречи и дела, меняет графики работы и передаёт текущие дела, собирает и упаковывает оборудование, оформляет командировки, покупает билеты, бронирует гостиницы и пр.

До начала работ DFIR компания, скорее всего, запросит у вас гарантийное письмо об оплате предстоящих работ и предложит заключить соглашение о конфиденциальности (NDA). С вашей стороны будет разумно уточнить заранее ставку часа работы эксперта DFIR. Подготовку гарантийного письма лучше осуществлять вне поражённой инфраструктуры во избежание получения этой информации находящимися в ней злоумышленниками. Можно заранее составить шаблон такого гарантийного письма без указания конкретной компании. NDA также лучше заключить заранее с компаниями, к которым вы планируете обращаться. Однако решение о заключении NDA может быть принято вами и перед или даже в ходе DFIR, т. к. передача информации осуществляется от вашей компании в экспертную компанию, проводящую DFIR, заинтересованной стороной в заключении NDA являетесь вы и целесообразно не затягивать его

заключение. Также при заключении NDA еще до начала работ вам будет проще настаивать на вашей редакции или ваших правках к редакции NDA привлекаемой компании. В ходе DFIR настаивать на правках сложнее. Если у вас (вашего менеджмента, акционера, директора по ИБ и т. д.) с этой компанией хорошие отношения, то этот шаг по договорённости может быть пропущен для экономии времени и скорейшего начала проведения DFIR. Также в этом случае у вас, скорее всего, уже заключен NDA с экспертной компанией.

## Как проходит офлайн (выездной) DFIR?

Эксперты приезжают в назначенное им место в согласованные дату и время с собственной техникой (ноутбуки, блокираторы записи, HDD для копий дисков и т. д.), проводится установочная встреча, затем анализ скомпрометированных узлов, поиск способа входа в инфраструктуру, всех поражённых узлов, закладок (RAT), анализ HDD и/или снятие с них копий с использованием блокираторов записи и т. д. Работа в небольших инфраструктурах происходит, как правило, с участием 1-2 экспертов в течение нескольких дней до подготовки чернового варианта отчёта (т. е. не считая время на последующую подготовку чистового отчёта). В случае двух экспертов DFIR работа, как правило, осуществляется в режиме 24x7: 8 часов эксперт DFIR работает в одиночку, 8 часов – вдвоем с напарником, 8 часов – отдых. Т. е., как правило, 8 из 16 рабочих часов в сутки оба эксперта работают совместно, 8 часов – поодиночке. Для более крупных инфраструктур может привлекаться больше экспертов DFIR – рекомендуем обсудить желаемые сроки проведения DFIR на старте работ, т. е. до выезда экспертов. Со стороны принимающей стороны требуется обеспечить как минимум аналогичный режим работы сотрудников IT и ИБ для максимально эффективного взаимодействия. В противном случае DFIR будут длиться дольше, но это время работы экспертов DFIR всё равно будет учитываться в трудозатратах для оплаты.

Следует отметить, что некоторые экспертные компании практикуют выездные работы только в исключительных случаях, считая онлайн-работу более эффективной, что, правда, не исключает возможность выезда одного специалиста для оказания помощи пострадавшей компании в сборе триажей/образов и т. п. для их передачи в лабораторию экспертной компании. Об онлайн (без выезда) DFIR будет подробнее указано ниже.

## К прибытию экспертов по DFIR необходимо приготовить/организовать:

- Рабочие места для экспертов (стол, стул, свет, электропитание).
- Создать чат ВНЕ корпоративного мессенджера с участием необходимых лиц (руководители IT и ИБ, представитель менеджмента, юрист, специалист службы маркетинга/PR). Критически важно, чтобы переписка в этом чате не могла быть прочитана злоумышленниками, включая потенциальных внутренних злоумышленников. Во-первых, доступ к этому мессенджеру должен быть в принципе исключён с узлов вашей инфраструктуры (включая удаление данного мессенджера с узлов сети, выход из сессий на рабочих устройствах и т. п.). Во-вторых, включайте в чат сотрудников только по явной необходимости.
- Во внутренней сети необходимо по вопросу инцидента соблюдать полную тишину и молчание, так как, скорее всего, злоумышленники читают всю вашу переписку в вашей корпоративной сети: почту (включая приглашения на собрания), ТКС/ВКС, корпоративные мессенджеры, личные мессенджеры, если в них был осуществлен вход в корпоративной сети. Режим молчания целесообразно соблюдать до получения отчёта о DFIR или до подтверждения возможности общения экспертами DFIR.
- Предусмотреть режим работы сотрудников IT и ИБ, синхронный с режимом работы экспертов DFIR.
- Предусмотреть отмену отпусков, командировок, увольнений задействованного в DFIR и последующем восстановлении и защите IT-инфраструктуры персонала (сотрудников IT- и ИБ-служб, руководителей и менеджеров, сотрудников для ввода информации с бумажных первичных документов (в случае утраты данных и резервных копий), инженеров (в случае нарушения работы АСУ ТП) и т. д.).
- Подумать о компенсациях для ваших сотрудников за переработки согласно ТК РФ (сверхурочные, отгулы, отпуск в будущем).

## Приблизительная длительность DFIR (реальность может отличаться от представленного ниже):

- Анализ 2-х HDD – один день.

| 100-200 узлов | 1000-2000 узлов | 50 тыс-150 тыс узлов |
|---|---|---|
| 1 неделя работы одного эксперта (100-500 рабочих часов) | 2 недели работы двух экспертов | 2 месяца работы сводных команд. |

Длительность DFIR напрямую зависит от того, на каком этапе была обнаружена атака, от применяемых злоумышленниками техник противодействия анализу и уклонения от защиты, а также от качества регистрации событий безопасности, состояния инфраструктуры и данных при обнаружении атаки. Например, в случае обнаружения атаки в фазе её начального развития период локализации инцидента и выявления точки входа может занять несколько часов, а в случаях, когда злоумышленники добрались до этапа разрушительного воздействия на IT-инфраструктуру, расследование может занять до нескольких дней, т. к. может потребоваться восстанавливать криминалистически важные данные из побитово (RAW) снятых образов дисков зашифрованных серверов и рабочих станций.

## Как проходит онлайн DFIR (без выезда)?

Эксперты DFIR просят сотрудников IT и ИБ заказчика выполнить те или иные действия по сбору улик, логов (обычно сбор осуществляется скриптами либо специальными программами) и прислать результаты для анализа экспертам. После изучения материалов экспертами процесс повторяется с новым заданием.

Онлайн IR по ставкам экспертов DFIR может быть на 20 - 30% дешевле, чем офлайн + не требуется учитывать к оплате время на прибытие и убытие, командировочные расходы.

Однако, если на стороне заказчика работ не будет слаженной, быстрой и экспертной работы, то суммарное время DFIR может оказаться больше, чем в случае офлайн работы – DFIR может продлиться дольше и в итоге оказаться даже дороже, чем офлайн вариант. Эксперты DFIR часто отмечают медленное выполнение сотрудниками компании заказчика поручаемых им задач и зачастую — рассинхронизацию по времени совместной (одновременной для экспертов DFIR и специалистов заказчика) работы в течение суток.

Таким образом, очень важно, чтобы в процессе реагирования на стороне пострадавшей компании была команда IT, способная оперативно идентифицировать ту или иную систему, собрать с неё необходимые данные, а также быстро применять получаемые рекомендации.

**В конце работ по DFIR**, т. к. эксперт DFIR формально не имеет права забирать в собственное пользование экземпляры обнаруженного вредоносного ПО, целесообразно прислушаться к его рекомендации загрузить вашими силами экземпляр вируса на предложенную экспертом площадку анализа файлов на вирусы (например, на отечественный https://virustest.gov.ru/) в целях его автоматического внесения в антивирусные базы. Возможно, этим вы спасёте кого-то или многих. Важно делать это **только после завершения DFIR**, так как вирус может содержать информацию об именно вашей организации, и его размещение на общедоступном ресурсе анализа вирусов может привести к раскрытию факта атаки на компанию. Если вы не хотите загружать образец вируса на общедоступный ресурс, спросите эксперта, куда он порекомендует направить образец вируса на анализ для выработки IOC для их включения в антивирусные базы в обезличенном виде.

**Оплата услуг по DFIR** осуществляется, как правило, после получения отчёта с требуемым заказчику уровнем детализации. Эксперт DFIR по вашему запросу дополнит первую финальную версию отчёта нужной вам детализацией и посчитает дополнительные потраченные на такое дополнение отчёта часы работы. Схема оплаты часто выглядит так: отчёт готов -> заказчик утверждает отчёт -> заключается договор -> производится оплата. Именно поэтому до начала DFIR компания может попросить у вас гарантийное письмо.

Оплата услуг DFIR осуществляется, как правило, из резервного бюджетного фонда генерального директора компании. Редки случаи, когда компания планирует резервы на проведение DFIR в рамках планового годового бюджета на ИБ. Хотя это ничему не противоречит, но требует определённой смелости директора по ИБ, чтобы заявить такую статью расходов, и зрелости понимания рисков в компании со стороны генерального директора, чтобы такую статью расходов подтвердить.

В целях планирования вы можете заранее заключить рамочное соглашение с одной или несколькими экспертными компаниями и определить расценки на период. В качестве альтернативы вы также можете купить подписку на сервис, выкупив заранее определённое количество часов и зафиксировав расценки. Выкупленные, но не потраченные часы экспертные компании, как правило, могут перевести в работы по Compromise assessment или в обучение ваших работников, или во что-то ещё, о чём вы можете договориться заранее при приобретении подписки. Как правило, заключение рамки позволяет частично снизить расходы на оплату услуг экспертов, а приобретение подписки — снизить ещё более. В целом, приобретение подписки или заключение рамочного договора со стороны, например, головной компании холдинга в интересах всех компаний холдинга может выглядеть хорошим решением. Возможно, также со временем появятся соответствующие страховые продукты для компаний – вы можете уточнить в вашей страховой. Подписка на сервисы по реагированию от «Лаборатории Касперского», например, предоставляет следующие преимущества:

- Оказание по запросу в гарантированные сроки
- Наличие выделенной телефонной линии, доступной 24/7
- Доступен перезачёт стоимости неиспользованной лицензии в счёт оплаты других решений «Лаборатории Касперского»[1]

## Рекомендуемые действия после получения отчёта DFIR

В ходе или после проведения DFIR и после согласования с юристами вашей компании может быть принято решение осуществить обращение в правоохранительные органы. Для этого юрист пострадавшей компании уже в процессе DFIR готовит заявительные материалы. Можно обращаться в правоохранительные органы после получения отчёта о DFIR, можно ещё в процессе DFIR или даже до его начала – это компания решает самостоятельно. Отчёт о DFIR может быть предоставлен в правоохранительные органы впоследствии, но крайне желательно – до вынесения решения о возбуждении уголовного дела или об отказе от его возбуждения. Правоохранительные органы самостоятельно примут решение, возбуждать уголовное дело или нет, на основании представленной информации и собственных выводов. Поэтому, если компания хочет получить и представить в правоохранительные органы отчёт экспертов DFIR для возбуждения уголовного дела, может быть целесообразно отложить подачу заявления в правоохранительные органы до получения отчёта. С указанными материалами и доверенностью на представление интересов компании в правоохранительных органах юрист компании обращается обычно в РОВД/ОВД по месту регистрации компании (в случае компании федерального значения иногда может быть целесообразно обращение выше – например, в ГУВД, СК или УБКП).

При первом обращении юрист получит первую справку – талон-уведомление о том, что заявление принято. У талона будет уникальный в рамках даты номер (КУСП). Рекомендуем всегда обращаться в правоохранительные органы, в том числе потому, что без КУСП активный поиск злоумышленников с помощью отдельных мер может быть незаконен.

В течение 30 дней после подачи заявления компания получит вторую справку о том, что следователь согласен с тем, что имело место преступление и возбуждено уголовное дело. Либо компания получит отказ (что довольно плохо для компании; причиной отказа может быть, например, непредоставление отчёта об инциденте или иных необходимых доказательств, на основании которых можно возбудить уголовное дело и признать пострадавшую компанию потерпевшей стороной). Рассмотрим процесс взаимодействия со следствием немного подробнее.

Для возбуждения уголовного дела инцидент должен иметь признаки состава преступления, например:

- Статья 158 УК РФ (Кража)

Кража представляет собой тайное хищение чужого имущества, в том числе денежных средств и иных материальных ценностей. В некоторых случаях применяется в отношении инцидентов в дистанционном банковском обслуживании (ДБО) или хищений с банковских карт (пункт «г» части 3 статьи 158 УК РФ), хотя в современных реалиях существуют специальные статьи для данных преступлений. Ключевым признаком состава преступления является тайное изъятие имущества без взаимодействия с потерпевшим.

- Статья 159 УК РФ (**Мошенничество**)

Основным признаком мошенничества является обман потерпевшего с целью хищения его имущества или получения имущественных прав. В современных условиях особой распространённостью пользуются:

- Статья 159.3 УК РФ (**Мошенничество с использованием электронных средств платежа**);
- Статья 159.6 УК РФ – мошенничество в сфере компьютерной информации.

В частности, статья 159.6 УК РФ охватывает хищение имущества или получение права на него путём несанкционированного вмешательства в функционирование компьютерных систем, хранения, обработки или передачи данных.

- Статья 163 УК РФ (**Вымогательство**)

Преступление образуется при предъявлении преступниками требований имущественного характера под угрозой совершения действий, которые могут причинить значительный вред правам или законным интересам потерпевшего. В контексте киберпреступности применяется, например, при использовании программ-вымогателей. Одной лишь записки от вредоносного ПО недостаточно – необходимо зафиксировать переписку между злоумышленником и потерпевшим, содержащую чёткие требования и угрозы.

- Статья 183 УК РФ (**Незаконное получение и разглашение коммерческой, налоговой или банковской тайны**)

Применяется в случаях незаконного сбора или распространения информации, содержащей коммерческую, налоговую или банковскую тайну. Может использоваться в делах, связанных с пробивами данных или утечками информации.

- Статья 187 УК РФ (**Неправомерный оборот средств платежей**)

Данная статья охватывает преступления, связанные с кардингом. Может применяться в случаях обнаружения скимминговых устройств. При этом само производство или оборот специальных технических средств для незаконного доступа к информации (например, скиммеров) может дополнительно квалифицироваться по статье 138.1 УК РФ, что требует проведения соответствующих экспертиз.

- Статья 272 УК РФ (**Неправомерный доступ к компьютерной информации**)

Преступление квалифицируется, если в результате неправомерного доступа к информационной системе зафиксированы: уничтожение, блокирование, модификация, копирование компьютерной информации.

Важно также установить общественно опасные последствия. Вопрос правомерности доступа определяется в соответствии с Постановлением Пленума Верховного Суда РФ от 15.12.2022 № 37. Данная статья часто применяется в сочетании с другими статьями (например, 159.6 или 273 УК РФ). В частности, DDoS-атаки подпадают именно под действие статьи 272 УК РФ.

- Статья 272.1 УК РФ (**Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации**)

Устанавливает уголовную ответственность за: незаконные использование, распространение, предоставление, доступ, сбор, хранение компьютерной информации, содержащей ПД, полученной путём неправомерного доступа к средствам её обработки, хранения, иного вмешательства в их функционирование, иным незаконным путём.

Статья 273 УК РФ (**Создание, использование и распространение вредоносных компьютерных программ**)

Преступление квалифицируется при наличии заключения эксперта или специалиста о том, что программное обеспечение является вредоносным и использовалось с преступной целью. Из-за сложности доказывания применяется редко, и зачастую расследуется в связке с другими статьями (например, 159.6, 272 УК РФ). Самостоятельное возбуждение дел по статье 273 УК РФ встречается крайне редко.

- Статья 274 УК РФ (**Нарушение правил эксплуатации средств хранения, обработки или передачи информации и информационно-телекоммуникационных сетей**)

Данная статья практически не применяется, так как для её реализации требуется совокупность условий:

- Наличие должностных инструкций и правил работы с техникой;
- Подтверждённое нарушение этих правил;
- Причинение крупного ущерба (свыше 1 млн рублей).

- Статья 274.1 УК РФ (Неправомерное воздействие на критическую информационную инфраструктуру РФ)

Применяется, если потерпевший входит в перечень объектов критической информационной инфраструктуры (КИИ). Включает в себя элементы состава преступлений, предусмотренных статьями 272 и 273 УК РФ, при этом к объектам КИИ предъявляются особые требования к безопасности.

Вы можете самостоятельно подготовить отчёт о расследовании и реагировании для его направления в правоохранительные органы, но вам необходимо будет изложить в отчёте все факты объективной стороны преступления, контрольные суммы файлов вредоносных программ (вот для этого и бывает нужен DF – чтобы восстановить удалённые злоумышленниками использовавшиеся ими программы), перечислить функциональные возможности выявленных вредоносных программ с указанием признаков, которые, по вашему мнению, можно отнести к вредоносному программному обеспечению (например, такие как уничтожение или блокирование информации – см. ст. 273 УК РФ), необходимо быть готовыми предоставить следствию сами вредоносные программы на флешке и так далее (**инструкция по сбору и сохранению технических данных для правоохранительных органов представлена ниже**). Всё, что указано в отчёте, должно быть воспроизводимо, например, должны быть указаны контрольные суммы, использованные программы с их версиями и т. д. Детальные требования к отчёту (что должно в нём быть) можно найти в соответствующей методичке МВД, изданной МосУ МВД России имени В.Я. Кикотя.

В процессе рассмотрения заявления компании будет определён следователь, который будет вести дело. Следователь с постановлением на выемку обратится в компанию и предложит предоставить свидетельства инцидента в виде выемки, очно, под протокол и видеосъёмку, после чего предоставленные свидетельства станут вещественными доказательствами в деле. Крайне важно, чтобы следователь после выемки признал пострадавшую компанию потерпевшей стороной и возбудил дело (пусть и против неустановленного пока круга лиц). В дальнейшем целесообразно, чтобы данный вывод подтвердил суд. Для возмещения убытков целесообразно стремиться к тому, чтобы совершившие атаку лица были найдены и признаны виновными на основании вступившего в законную силу решения суда, а компания была признана потерпевшим в уголовном деле. Это позволит предъявить иск о возмещении причинённого преступлением вреда (ст. 42 Уголовно-процессуального кодекса РФ). При этом установление виновных в атаке лиц не снимает с компании и её уполномоченных работников ответственность в случае нарушения ими правил защиты информации (например, правил эксплуатации критической информационной инфраструктуры).

Пострадавшая компания может периодически обращаться к следователю с просьбой о доступе к уголовному делу (в отношении информации только своего юридического лица) для отслеживания прогресса.

Дальнейшей задачей следствия является, если упростить, установить третье лицо (злоумышленника), подать его в розыск, задержать, направить дело в суд.

Когда злоумышленник будет признан виновным, потерпевшие смогут предъявить к нему претензии в суде.

В числе прочего справка о признании компании потерпевшей и о возбуждении уголовного дела необходима для ряда государственных органов, например, для ФНС, если была утрачена или зашифрована бухгалтерия компании. Так ФНС вполне может подать на компанию в суд за несвоевременное или неполное предоставление очередной бухгалтерской отчётности и соответствующая справка может помочь компании получить отсрочку в предоставлении отчётности (справка подтвердит в суде, что компания не сама удалила (скрывает) свою бухгалтерию).

# Шифрование или удаление данных – это ещё не все проблемы. Утечка данных

Возможно, в ходе инцидента, ещё до шифрования данных, у вас украли изрядную долю информации. Определить это часто можно по журналам сетевых средств защиты или статистике исходящего трафика в сторону сети интернет, а также по отдельным следам, выявленным в ходе реконструкции событий инцидента. Злоумышленники могут попросить у вас выкуп за её удаление, но нет гарантий, что они это сделают, а если вы не платили выкуп за расшифрованные данных – то нет гарантий вдвойне.

Поэтому ваши данные, скорее всего, будут проданы всем готовым за них хоть сколько-то заплатить.

В украденных у вас данных могут быть, например:

- Ключи и пароли от ваших личных кабинетов во внешних сервисах, включая государственные учреждения, сервисы партнёров и т. д.
- Персональные данные ваших сотрудников и клиентов.
- Информация о вашей экономической деятельности, договорах и т. д.
- Ваша интеллектуальная собственность: разработанный программный код и т. п.

Целесообразно сменить ключи и пароли от ваших личных кабинетов во внешних сервисах в ходе или сразу после завершения DFIR, а в сервисах проверить состав операций и пользователей, т. к. злоумышленники могут создать дополнительные аккаунты для доступа к таким вашим личным кабинетам.

Через какое-то время после продажи ваших данных или если на них не найдётся покупатель, они, вполне вероятно, будут порциями или целиком опубликованы в открытом доступе. Вы можете столкнуться с обращениями клиентов и партнёров, а также правоохранительных органов. Если вы ранее не уведомили все необходимые правоохранительные органы, например, Роскомнадзор, об утечке персональных данных, вам необходимо будет выполнить соответствующие мероприятия в установленный законом срок.

В будущем могут быть опубликованы новые порции ранее украденных у вас данных и выданы за новую утечку — вам необходимо быть готовыми проанализировать такие данные (путём сравнения со старыми и с текущими актуальными данными), чтобы либо подтвердить, что это старая утечка, либо снова проводить DFIR либо CA (о CA будет ниже), если есть признаки новой утечки информации (например, если данные актуальны и содержат те уникальные данные, которых у вас не было на момент прежней утечки и которые злоумышленники не могли взять у кого-то другого и «добавить» к вашим старым данным).

Для возможности оперативного сравнения данных из новых утечек из ваших систем целесообразно сохранить в виде отдельной БД ранее украденные/опубликованные злоумышленниками данные либо срез реальных данных на момент утечки.

В случае утечки персональных данных (ПДн) необходимо уведомить уполномоченные государственные органы:

**24 часа**

с момента выявления утечки ПДн – уведомить Роскомнадзор.

**72 часа**

с момента выявления утечки ПДн – направить в Роскомнадзор отчёт о результатах внутреннего расследования.

- Субъект КИИ – в 24 часа уведомить НКЦКИ (формат ГосСОПКА).
- Поднадзорный ЦБ РФ – направить уведомление посредством АСОИ ФинЦЕРТ в Банк России.
- Если утечка произошла в результате хакерской атаки, то оператор ПДн обязан направить информацию в ГосСОПКА о компьютерном инциденте, повлекшем неправомерную передачу ПДн.
- Органы по линии GDPR (если ваша компания по каким-то причинам соблюдает GDPR).

Чтобы своевременно выполнить обязанности по информированию государственных органов, целесообразно заранее в отношении каждого информируемого органа власти:

- Изучить порядок информирования и требования к форме и составу данных.
- Определить основные и резервные каналы информирования и порядок фиксации получения уведомления.
- Получить и периодически проверять (поддерживать) доступ к личным кабинетам (в случае дистанционного информирования).
- Учесть филиальную сеть вашей организации/группы/холдинга.
- Определить ответственных за составление, согласование и направление отчётов в государственные органы.
- Определить порядок информирования субъектов ПДн об утечке и размещения информации/пресс-релизов об утечке в открытых источниках, доступных субъектам.
- Определить ответственных за составление, согласование и публикацию информации/пресс-релизов.
- Согласовать заранее шаблоны пресс-релизов.

## Что делать, если у вас есть подозрение, что вашу IT-инфраструктуру взломали и могут зашифровать и уничтожить, но этого ещё не произошло?

Что может быть таким основанием:

- Ощущение некорректной работы IT-инфраструктуры, например, ввиду происходящих в ней с административными правами изменений, не санкционированных вами.
- Наличие уязвимого ПО или сервисов на внешнем (интернет) периметре, которые вы не устраняете оперативно.
- Отчёт о тесте на проникновение с успешной компрометацией вашей компании.
- Имеются подозрения на компрометацию инфраструктуры.
- И многое другое...

В данной ситуации целесообразно:

- Провести CA (Comromise Assessment – поиск следов взлома).
- Проверить безопасность, целостность и доступность ваших бэкапов (резервных копий данных), а также самой системы резервного копирования.
- Рассмотреть рекомендации в приложениях 1 и 2 ниже.

CA (Compromise Assessment) — выявление признаков компрометации (в ситуации, когда нет очевидных следов / признаков взлома / инцидента) до того, как они приведут к серьёзным последствиям. Содержит проверку всей IT-инфраструктуры, включая сканирование сети, сбор и анализ доказательств – это могут быть терабайты данных и недели на сбор и анализ данных. Целью CA является обнаружение признаков несанкционированного доступа, нелегитимной активности и скрытых угроз, которые могут оставаться незамеченными, в т. ч. для СЗИ, длительное время. При обнаружении угроз позволяет локализовать их, лишить злоумышленников возможности взаимодействия со скомпрометированными системами и, если возможно, установить причины их возникновения.

«Лаборатория Касперского» предоставляет сервис Kaspersky Compromise Assessment, обнаруживающий активные кибератаки и ранее неизвестные угрозы, которым удалось обойти имеющиеся средства и процессы информационной безопасности. Подробнее ознакомиться с сервисом и оставить заявку можно здесь.

Обычно CA проводится дольше, чем DFIR, и в более спокойном режиме (т. к. нет факта прерывания деятельности компании), а если нет ограничений с вашей стороны или со стороны вашего регулятора, то зачастую и в удалённом (online) режиме.

Основной задачей CA является полное и длительное изучение инфраструктуры и коммуникаций, т. к., в отличие от свершившегося инцидента IT, нет «ниточки», которую можно бы было раскручивать, а злоумышленники, если они проникли в инфраструктуру компании, на данном этапе стараются скрывать следы своего присутствия. При проведении CA также следует соблюдать режим тишины о проводимых мероприятиях: злоумышленник, при его обнаружении, может запустить шифрование или удаление инфраструктуры.

Некоторые компании для проведения CA предлагают использовать ПО собственной разработки, такое как EDR/XDR или MDR. Последнее (MDR), как правило, имеет постоянную связь с облаком своего поставщика и передаёт туда все подозрительные данные для анализа специалистами сторонней компании, что может накладывать определённые ограничения на возможность применения вами этого решения.

## Приложение 1. Из каких шагов состоит сам DFIR

6 основных шагов IR (подробнее см. в методичке SANS и в Руководстве по работе с инцидентами компьютерной безопасности – NIST Computer Security Incident Handling Guide – перевод последней есть на altx-soft.ru):

### Этап 1. Подготовка к будущему инциденту.

Если вы заранее не проверили возможность выполнения указанных ниже в данном разделе мероприятий, то вам, скорее всего, придётся учиться это делать в процессе DFIR, что негативно повлияет на длительность DFIR и его стоимость, а также на его результаты.

1. Реализация политики хранения логов:
   a) Настройка ведения журналов (логов) с достаточной детализацией.
   b) Обеспечение безопасного хранения журналов (логов) — например, на удалённом SIEM или на отделённом от инфраструктуры сервере.
   c) Настройка длительности хранения журналов (логов).
2. Обеспечение возможности физического доступа к содержимому каждого диска (HDD) с данными в компании с обеспечением возможности:
   a) Взять диск в руки.
   b) Расшифровать диск (если он зашифрован самой компанией в целях безопасности).
3. Обеспечение возможности доставать артефакты:
   a) Сетевой доступ ко всем узлам.
   b) Административные права для доступа ко всем узлам.
   c) Хранение реквизитов доступа (паролей) для административного доступа ко всем узлам безопасным с точки зрения уничтожения образом (например, на бумаге в противопожарном сейфе).
4. Обеспечение наличия резерва оборудования, вычислительных мощностей и дискового пространства для временного или постоянного развертывания IT-инфраструктуры или её части без отключения заражённых (взломанных) узлов, потребляющих ресурсы. Это может быть просто резерв мощности и дисков в системе виртуализации или договор на облачный IaaS с пониманием способа безопасного доступа туда и порядка и стоимости масштабирования.
5. Обеспечение удалённого хранения резервных копий и данных (согласно правилу резервного копирования «3-2-1», где ключевое для данного документа – это хранение одного экземпляра резервных данных вне вашей инфраструктуры).

### Этап 2. Идентификация того, что инцидент произошел.

1. Вам необходимо знание того, куда смотреть, чтобы понять, что инцидент начался. Например:
   a. Источники Threat Intelligence фидов с данными о возможной подготовке атаки на вашу компанию (например, регистрация фишинговых доменов, объявления о покупке или продаже доступа в вашу сеть и т. д.).
   b. SIEM/SOC.
   c. MDR.
   d. Централизованный (!) EDR/XDR.
   e. Централизованный (!) AV.
   f. Система IT-мониторинга для контроля работоспособности и выявления отключения средств защиты.
   g. Экран зашифрованного компьютера (если вы не озаботились пунктами выше).
   h. Телеграм-каналы с данными о взломах и утечках (вы одним из первых прочтёте про свою компанию по пути на работу, пока в офисе ещё никого нет, но всё уже зашифровано или удалено...).

### Этап 3. Изоляция выявленного поражённого злоумышленниками IT-парка оборудования.

1. НЕ отключать электропитание!
2. Отключать от ЛВС:
    a. Виртуальные машины – на уровне системы управления виртуализацией отправить в «down» сетевой интерфейс (все сетевые интерфейсы ВМ).
    b. Физические машины – вынуть сетевой провод из сетевой карты (RJ45 или оптику). Или вынуть провод на свиче. Или погасить порт на свиче.
    c. Wi-Fi – погасить сетевой интерфейс в ОС. Или погасить Wi-Fi точку доступа. Или на точке доступа заблокировать узел по MAC (в случае уверенности, что злоумышленник не имеет доступа к узлу по другим интерфейсам + сменить пароль Wi-Fi на случай автоматической смены MAC узла зловредной программой).
    d. SAN сеть (СХД, т. к. запущенный на виртуальной/физической машине процесс может продолжать шифровать данные на подключенной СХД).

### Этап 4. Зачистка.

1. Удаление троянов/закладок/web-шелов/RAT и т. д.
2. Установка обновлений безопасности для устранения уязвимостей, включая новейшие обновления (могут закрывать ещё не опубликованные, но уже известные злоумышленникам уязвимости).
3. Установка и настройка средств защиты (как правило, отключаются или «портятся» злоумышленниками).
4. Смена паролей. Включая все системные УЗ. Включая в домене. И локальные. И в СУБД. И в VPN. И в прикладе. Вообще все. Для Kerberos необходимо сменить пароль дважды. И ключи SSH/SSL тоже. И сертификаты web-сервисов. И пароли и ключи в ДБО вашего банка.

### Этап 5. Восстановление.

1. Восстановление из резервных копий.
2. Включение ранее отключенных сетевых интерфейсов.

### Этап 6. Выводы.

1. Отчёт об инциденте и реагировании.
2. Рекомендации для неповторения инцидента -> план работ.
3. Всё работает!

## Приложение 2. Меры подготовки к будущим инцидентам ИБ

При подготовке к возможному будущему инциденту с шифрованием/удалением/кражей данных стоит разделить подготовительные мероприятия на два вида и рассматривать инвестиции в них раздельно:

- Мероприятия и инвестиции **в области минимизации вероятности ущерба** – это сокращение поверхности атаки, настройка (харденинг) IT-инфраструктуры, внедрение и настройка СЗИ, мониторинг и т. д. Данным мероприятиям посвящено много стандартов и статей в области ИБ, они сильно зависят от масштабов, технологий, истории компании и могут быть проведены с привлечением компетентного подрядчика, имеющего соответствующую лицензию на работы в области защиты информации. В данных методических рекомендациях данный вопрос практически не затрагивается ввиду большого количества доступной на рынке и в сети интернет информации по данному вопросу. В основном данные меры направлены на то, чтобы затруднить злоумышленникам атаку на вашу IT-инфраструктуру, заставить их дольше проводить разведку и оставить больше следов (по которым вы можете раньше почуять неладное).
- Мероприятия и инвестиции **в области минимизации размера ущерба при инциденте** – данные методические рекомендации и, в частности, данное приложение к ним дают некоторый набор мероприятий, которые целесообразны к рассмотрению и реализации в целях сокращения времени проведения DFIR и восстановления и, как следствие, в целях сокращения времени простоя в работе пострадавшей компании и сопутствующих и последующих расходов.
- Чтобы быстрее провести DFIR или CA и, соответственно, быстрее восстановить вашу IT-инфраструктуру и данные, целесообразно заранее оценить уровень вашей кибербезопасности и принять в том числе следующие меры подготовки к будущим инцидентам взлома вашей IT-инфраструктуры злоумышленниками, преследующими цели её шифрования или удаления.

### Для сокращения времени реагирования и восстановления рекомендуем предусмотреть заранее:

- Контакты сервисных компаний по реагированию на киберинциденты. **Заказать расследование у «Лаборатории Касперского» можно по ссылке**. Согласованный порядок взаимодействия, лимит согласованных расходов, полномочия у потенциальных подписантов NDA и гарантийных писем для начала проведения DFIR. Шаблоны гарантийных писем и NDA, готовность крайне быстро внести в них изменения без длительного согласования.
- Назначение ответственных (и замещающих их) лиц за реагирование в такой ситуации. В первую очередь это лица, отвечающие за единоличное принятие решений, внешние коммуникации, организацию и проведение DFIR. Обеспечение наличия под рукой всех их необходимых контактов, вплоть до номеров телефонов родственников, для возможности найти и связаться с ответственными работниками в любое время. Назначение дежурного лица (как правило, из числа IT и ИБ) на внерабочее время пятницы, на выходные и на праздничные дни.
- Проведение хотя бы штабных учений, в ходе которых следует убедиться в понимании ответственными лицами своих ролей, последовательности действий, наличия необходимых инструментов, ресурсов и возможностей.
- Проверку возможности выполнить всё, указанное в Приложении № 1, особенно указанное в составе Этапа 1.
- Правило резервного копирования «3-2-1» (три резервные копии на двух разных носителях, один из которых находится вне предприятия).
- Проверить возможность восстановления данных и систем (т. е. также и программ), проверить корректность работы систем после восстановления данных.
- Безопасность самой системы резервного копирования (СРК) и бэкапов не должна зависеть от компрометации службы каталогов AD. Полезно рассмотреть отдельные не доменные учётные записи для работы с СРК или многофакторную аутентификацию. Полезно использовать отдельный АРМ (вне AD) для работы с СРК, отдельные сетевые сегменты для такого АРМ и отдельные для СРК, или хотя бы разместить резервные копии на сервере с ОС другого семейства и вне AD/LDAP в отдельном сетевом сегменте.
- Запись паролей на бумажный носитель и размещение его в сейфе (либо размещение в сейфе носителя с зашифрованным файлом с паролями, который при необходимости может быть подключен в режиме read-only).

- Составление карты сети с указанием точек подключения к интернет и узлов (сетей), взаимодействующих с интернетом. Периодическая выгрузка записей внутреннего DNS в файл и на внешний носитель.
- Внедрение SIEM и построение на его базе SOC, либо подключение вашей IT-инфраструктуры к внешнему SOC.
- Внедрение MDR (как временное решение в отсутствие SOC или дополняющее SOC). С этим вопросом может помочь решение «Лаборатории Касперского» Kaspersky MDR, которое повышает уровень информационной и технической безопасности небольших организаций с невысоким уровнем ИБ-экспертизы за счет быстрого развертывания услуги «под ключ». Подробнее с решением можно ознакомиться здесь.
- Настройку правил аудита (журналирования, логирования) событий безопасности и глубины (длительность) хранения журналов.
- Безопасное хранение журналов аудита (недоступно для злоумышленников при взломе вашего AD или вне вашей инфраструктуры) – например, внешний SOC или DataLake.
- Исключить подключение носителя с ключами ДБО (интернет-банка) к компьютеру, кроме выполнения действия по подписанию документов. Да, это не так удобно, зато, когда бухгалтер отходит от компьютера, злоумышленник не подпишет и не отправит несанкционированный платёж.
- Средства коммуникации между сотрудниками и с сервисной (DFIR) компанией при инциденте, исключающие чтение переписки злоумышленниками, то есть вне поражённой инфраструктуры.
- Ответственные за коммуникации при инциденте и согласованные шаблоны-заготовки (кому и о чём сообщить) для:
  - коммуникации с руководством, СД, акционерами;
  - коммуникации с техническим персоналом и сервисными компаниями;
  - коммуникации с работниками;
  - коммуникации с клиентами;
  - коммуникации с госорганами.
- Инструменты и методы для сетевой изоляции поражённых хостов, включая физические и виртуальные, пользовательские и серверы – как вы будет их отключать от сети? Сколько это займёт времени? Кого и как предупредить об отключении узла с тем, что какой-то процесс остановился и что нельзя включить узел в вычислительную сеть обратно и нельзя отключать электропитание?
- Инструменты для отключения сети организации от сети интернет: полностью, а также частично, по «белому» списку проверенных адресов контрагентов, включая ведение таких списков, и аналогично по «чёрному» списку (включающему известные файлообменники, ресурсы в иных странах, не связанных с клиентской базой, облачных провайдеров типа Amazon и т. п.).
- Преднастроенные, но не активированные ACL на МСЭ, позволяющие изолировать заражённые сетевые сегменты (проекты, бизнес-направления, среды и т. д.) на время реагирования, с сохранением минимально необходимых входящих в такие сегменты сетевых доступов со стороны средств защиты.
- Средства выявления эксфильтрации и скачивания данных или хотя бы выявления нестандартного большого исходящего в сеть интернет-трафика.
- Инструменты анализа перечня запущенного ПО и его избирательной блокировки.
- Инструменты массового распространения, запуска и удаления нужных вам файлов и каталогов.
- Инструменты, дистрибутивы и экспортированные настройки для возможности развёртывания поражённого узла из образа или с помощью дистрибутива.
- Запрет входящего сетевого взаимодействия однотипных узлов внутри VLAN, например, терминальных серверов или рабочих станций, кроме случаев, когда это не связано с задачами управления и нет возможности вынести узел управления в отдельный сегмент.
- Мониторинг отключения VolumeShadow Copy Service под Windows и отключения СЗИ либо изменения их конфигурации (в т. ч. внесения ВПО в исключения) для раннего обнаружения злоумышленников.
- Инвентаризацию узлов сети, проверку наличия на них средств защиты и мониторинг отключения таких СЗИ.
- Подключение источника или источников TI-фидов или сервиса класса DRP (защита бренда в цифровом мире) для выявления подготовки атак и/или продажи доступа или данных организации.

## Материал опубликован на базе рекомандаций версии 1.0.2

Рекомендации подготовлены на основе личного опыта и разрешены к распространению по лицензии BSD 4-Clause с обязательным указанием версии и ссылки на автора, т. к. регулярно дополняются с учётом актуального опыта профессионального сообщества. Рекомендации не могут быть абсолютно применимы для всех возможных случаев и не могут гарантировать идеального результата действий при реагировании на инцидент ИБ.

Рекомендации разработаны Константином Титковым, руководителем Центра ИБ дочерних и зависимых обществ, Газпромбанк, при поддержке ряда экспертов отрасли ИБ. В первую очередь это:

Сергей Голованов, соавтор

Илья Зуев, соавтор

Антон Величко

а также коллеги, которые задавали вопросы и делились опытом на конференциях и после них.

Предложения по дополнению рекомендаций принимаются телеграммами по адресу @ktitkov.

**www.kaspersky.ru**