Swiss International Institute Lausanne

РУКОВОДСТВО ПО ПРОЦЕДУРЕ ПРИ ВЗЛОМЕ ДАННЫХ

Швейцарский международный институт Лозанны – SIIL

Утверждено:	Академическим советом
Дата утверждения:	01.09.2022
Дата пересмотра:	01.09.2025
Ответственный:	Отдел ИТ
Контактное лицо:	p.tkachev@siil.ch

Grand'Rue 92, 1820 Montreux, Switzerland
+41 31 520-70-82 • info@siil.ch • https://siil.ch

РУКОВОДСТВО ПО ПРОЦЕДУРЕ ПРИ ВЗЛОМЕ ДАННЫХ

Швейцарский международный институт Лозанны – SIIL

Содержание

I ВВЕДЕНИЕ

Согласно законодательству о защите данных, Швейцарский международный институт Лозанны – SIIL (далее «ВУЗ» или «SIIL») обязан обеспечивать безопасность и защищенность данных и оперативно принимать надлежащие меры в случае нарушения безопасности персональных данных (здесь и далее «взлома данных»).

В настоящем Руководстве по процедуре приведена структура информирования о взломе и реагирования на такие ситуации, если они касаются персональных данных, контролируемых и обрабатываемых ВУЗом. Инструкция дополняет *Политику по защите данных* SIIL, обеспечивающую готовность ВУЗа охранять права физических лиц на конфиденциальность в соответствии с законодательством Швейцарии о защите данных, а также, если применимо, Общим регламентом защиты персональных данных (GDPR).

Если взлом данных с большой вероятностью ставит под угрозу права и свободы субъектов данных, ВУЗ, согласно GDPR (если применимо), обязан сообщить об этом специалисту Департамента по защите данных **в течение 72 часов после обнаружения этого факта, даже если риск считается несущественным**.

Если применимо, меры по информированию субъектов взломанных данных и снижению рисков для их конфиденциальности в связи со взломом должны быть приняты незамедлительно, согласно статье 34 GDPR.

В указанный срок входят выходные дни и государственные праздники. Невыполнение этого правила грозит санкциями регулирующих органов и ущербом для репутации SIIL.

В связи с этим чрезвычайно важно принять меры немедленно, как только становится известно о взломе или возникает подозрение о происшествии, связанном с утратой или раскрытием данных. Необходимо незамедлительно связаться по электронной почте dpo@siil.ch со специалистом Департамента по защите данных и с начальником Департамента/ Отдела. В теме всех электронных писем по этому поводу должна стоять пометка «Срочно» (Urgent).

Если вы не уверены, является ли происшествие взломом данных, ознакомьтесь с инструкциями в настоящем документе и обратитесь за консультацией к специалисту Департамента по защите данных.

II ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящее Руководство касается физических лиц, обрабатывающих персональные данные от имени SIIL, в том числе:

- Всех физических лиц, трудоустроенных в SIIL или привлеченных SIIL и имеющих доступ к контролируемым или обрабатываемым SIIL персональным данным в ходе выполнения своих трудовых обязанностей или работы в административных, научно-исследовательских и/или иных целях;

- Всех студентов SIIL, имеющих доступ к контролируемым или обрабатываемым SIIL персональным данным в ходе обучения, в административных, научно-исследовательских и/или любых иных целях; или

- Физических лиц, не трудоустроенных в SIIL напрямую, но являющихся сотрудниками подрядных (или субподрядных) организаций и имеющих доступ к контролируемым или обрабатываемым SIIL персональным данным в ходе выполнения своих обязанностей для Института.

Настоящая Инструкция касается:

- Всех персональных данных, которые обрабатываются SIIL в любой форме (в том числе электронных и бумажных учетных данных), используются на рабочем месте (в том числе при работе из дома), хранятся на портативных устройствах и носителях информации, транспортируются с рабочего места в физической или электронной форме, а также данных, доступ к которым осуществляется удаленно;
- Персональных данных, находящихся во всех ИТ-системах и программных решениях SIIL, в том числе на облачных платформах, управление которыми осуществляется централизованно Отделом ИТ-услуг и поддержки или локально отдельными департаментами, отделами, институтами или центрами;
- Всех прочих ИТ-систем, в том числе платформ электронной почты и облачных платформ, где обрабатываются персональные данные, управлением или обработкой которых занимается SIIL.

III ОПРЕДЕЛЕНИЯ И ТЕРМИНЫ: ЧТО ТАКОЕ ВЗЛОМ ДАННЫХ?

Согласно GDPR и законодательству Швейцарии, в которое интегрирован GDPR, **взлом данных** определяется как нарушение безопасности, ведущее к случайному или незаконному уничтожению, утрате, изменению, несанкционированному раскрытию персональных данных или доступу к таким данным, передающимся, хранящимся или иным образом обрабатываемым. Под это определение подходят нарушения безопасности, вызванные злонамеренными действиями, недостатком

надлежащих средств контроля безопасности, отказом системы, отказом по вине человека или ошибками.

Взлом данных может происходить в разных ситуациях. Вот несколько примеров:

- Раскрытие конфиденциальных данных несанкционированным физическим лицам. Например, при случайной отправке электронного письма, содержащего конфиденциальные данные или данные непубличного характера, одному или нескольким получателям вследствие ошибки со стороны человека.
- Утрата или кража данных, в том числе оборудования, на котором хранятся эти данные (например, ноутбука, смартфона, планшета, USB-ключа и т.д.), либо записей в бумажной форме.
- Ненадлежащие средства контроля доступа, делающие возможным несанкционированное использование информации (например, загрузку персональных данных на незащищенный веб-домен, использование ненадежных паролей).
- Отказ оборудования.
- Случаи, когда конфиденциальная информация остается в незащищенном виде в местах, где к ней могут получить доступ посторонние лица (например, если владелец оставляет ИТ-оборудование без присмотра, не выйдя из аккаунта пользователя).
- Сбор персональных данных несанкционированными лицами.
- Действия хакеров, вирусы или иные атаки на ИТ-оборудование, системы или сети.
- Нарушение физической безопасности (например, взлом дверей, окон или шкафов для хранения документов).

Касается ли персональных данных происшествие, предположительно являющееся взломом данных, определяется индивидуально для каждого конкретного случая. Если происшествие не касается персональных данных, оно не является взломом данных, согласно определению GDPR. Более того, не все происшествия с данными, касающиеся персональных данных, считаются взломом данных.

Например, взломом данных не являются следующие случаи:

- Персональные данные надежно зашифрованы или анонимизированы таким образом, что ознакомление с ними невозможно; и/или
- Существует полная актуальная резервная копия персональных данных (при случайном уничтожении).

В случае каких-либо сомнений относительно того, произошел ли взлом данных, необходимо немедленно проконсультироваться со специалистом Департамента по защите данных.

Персональные данные определяются в GDPR следующим образом:
«Любая информация, касающаяся идентифицированного или идентифицируемого физического лица («субъекта данных»); идентифицируемое физическое лицо – это лицо, которое может быть прямо или косвенно идентифицировано, в том числе с помощью такого средства идентификации, как имя, номер удостоверения личности, данные о местоположении или онлайн-идентификатор, либо с помощью одной или более особых характеристик физической, психологической, генетической, умственной, экономической, культурной или социальной идентичности такого физического лица».

Особые категории персональных данных определяются в GDPR следующим образом:
«Персональные данные, указывающие на расовое или этническое происхождение лица, его политические убеждения, религиозные верования или философские взгляды; данные, касающиеся членства в профсоюзе, генетические и биометрические данные, которые обрабатываются в целях уникальной идентификации физического лица; данные, касающиеся здоровья, половой жизни или сексуальной ориентации физического лица».

Обработка определяется в GDPR следующим образом:
*«Любая операция или набор операций, выполняемых с персональными данными или массивами данных, будь то автоматизированными средствами или нет, например, сбор, запись, организация, структурирование, хранение, адаптация или изменение, получение, консультирование, **использование**, разглашение через передачу, распространение или доведение до сведения иным образом, гармонизация или объединение, ограничение, удаление или уничтожение».*

IV ПРОЦЕДУРА ИНФОРМИРОВАНИЯ О ВЗЛОМЕ ДАННЫХ

Согласно законодательству Швейцарии и в отличие от статьи 33 GDPR (когда применимо), предусматривающей конкретный 72-часовой срок, SIIL обязан уведомить о взломе данных специалиста Департамента по защите данных **как можно скорее**, если принято решение о необходимости информирования о происшествии.

В этот срок входят выходные дни и государственные праздники.

Согласно статье 34 GDPR, когда она применима, SIIL обязан проинформировать пострадавших лиц **без излишнего промедления**, если взлом данных с большой вероятностью ставит их конфиденциальность под серьезную угрозу.

Соответственно, по всем взломам данных необходимо немедленно принимать надлежащие меры. Если сотруднику SIIL становится известно о произошедшем, потенциальном или предполагаемом взломе данных, он/она обязан(а) немедленно сообщить об этом происшествии специалисту Департамента по защите данных по адресу dpo@siil.ch, а также своему руководителю

Департамента/ Отдела. В теме всех электронных писем по этому поводу должна стоять пометка «Срочно» (Urgent).

Специалист Департамента по защите данных отвечает за письменную фиксацию всех потенциальных или предполагаемых взломов данных, о которых его/ее уведомили.

V ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ ВЗЛОМА ДАННЫХ

Получив уведомление о взломе данных, специалист Департамента по защите данных должен совместно с соответствующими сотрудниками совершить следующие пять шагов (согласно лучшей практике) в рамках реагирования на происшествие:

- **Шаг 1. Определение и первоначальная оценка происшествия;**
- **Шаг 2. Локализация и восстановление;**
- **Шаг 3. Оценка рисков;**
- **Шаг 4. Уведомление;**
- **Шаг 5. Оценка и реагирование.**

1. Шаг 1. Определение и первоначальная оценка происшествия

Если любой сотрудник SIIL считает, что произошел или мог произойти взлом данных, он/она обязан(а) немедленно сообщить о происшествии специалисту Департамента по защите данных.

Специалист Департамента по защите данных проводит первоначальную оценку происшествия. При этом учитываются следующие факторы:

- Произошел ли взлом данных;
- Характер и тип персональных данных, безопасность которых была нарушена, в т.ч. наличие угрозы для данных непубличного характера или конфиденциальных персональных данных;
- Причина взлома;
- Масштаб взлома (т.е. количество пострадавших физических лиц);
- Потенциальный ущерб для пострадавших физических лиц;
- Меры, принятые для локализации взлома.

После первоначальной оценки происшествия специалист Департамента по защите данных может, в зависимости от степени серьезности происшествия, проконсультироваться с Ректоратом и принять решение о необходимости назначения группы заинтересованных сторон из SIIL (например, из Отдела ИТ-услуг, Финансового отдела, Отдела кадров, Отдела учета) для содействия расследованию и локализации.

2. Шаг 2. Локализация и восстановление

В случае взлома данных необходимо немедленно принять надлежащие меры для ограничения его масштаба.
Специалист Департамента по защите данных, проконсультировавшись с соответствующими сотрудниками:

- Определяет сотрудников SIIL, которых необходимо уведомить о взломе (например, Отдел ИТ-услуг и поддержки, Административный департамент) и о том, какую роль они должны сыграть в его локализации (например, изолировать скомпрометированную часть сети, уведомить пострадавших физических лиц);
- Определяет, можно ли принять какие-то меры для восстановления утраченных данных и ограничения ущерба от взлома;
- При необходимости уведомляет уполномоченные органы (например, в случае преступных действий).

3. Шаг 3. Оценка рисков

Специалист Департамента по защите данных совместно с соответствующими сотрудниками и на основании предоставленной информации выполняет свою обязанность по оценке потенциальных отрицательных последствий для физических лиц, в частности того, с какой вероятностью эти отрицательные последствия реализуются и насколько они будут серьезными или существенными.

В частности, в ходе такой оценки необходимо учесть вероятность реализации рисков и классифицировать серьезность этих рисков по категориям «Риск отсутствует», «Риск присутствует», «Высокий риск», согласно нижеприведенным критериям:

- **Характер взлома**. Уничтожение, повреждение или иной несанкционированный, случайный или незаконный доступ к персональным данным, их сбор, использование, запись, хранение или распространение. Взлом данных какого типа произошел или мог произойти? Нарушена ли конфиденциальность персональных данных? Стали ли персональные данные недоступны (временно или навсегда), возможен ли доступ к ним? Если это временное нарушение, сколько времени займет восстановление доступности или доступа?
- **Характер персональных данных.** Имеют ли персональные данные непубличный характер? Чем менее публичны персональные данные, тем выше риск при нарушении их безопасности. Более высокий риск для пострадавших физических лиц также может определяться полезностью соответствующей информации.
- **Масштаб и объем пострадавших персональных данных.** Как правило, чем больше объем зафиксированных персональных данных и число потенциально пострадавших физических лиц, тем выше риск.
- **Простота идентификации.** Простота идентификации физических лиц на основании их персональных данных с большой вероятностью повышает риск хищения личных данных, мошенничества и ущерба для репутации.

- **Меры безопасности.** Ограничены ли вызванные взломом риски благодаря внутренними мерам безопасности, таким как шифрование, если конфиденциальность ключа не пострадала, а третья сторона не в состоянии ознакомиться с данными?
- **Меры сдерживания.** Существуют ли меры сдерживания, делающие риск вследствие взлома данных маловероятным для пострадавших физических лиц?
- **Прочие факторы.** При оценке риска для пострадавших физических лиц следует также учитывать прочие релевантные факторы – наличие у физических лиц, пострадавших от взлома данных, особых характеристик (например, являются ли они детьми или взрослыми из уязвимых категорий).
- **Серьезность риска.** На основании вышеуказанных критериев и прочих релевантных факторов специалист Департамента по защите данных оценивает серьезность риска с точки зрения потенциальных последствий для физических лиц, пострадавших от взлома данных.
- **Вероятность реализации риска (рисков).** После взлома данных специалист Департамента по защите данных должен объективно оценить вероятность реализации потенциальных рисков, что является частью оценки рисков.
- **Оценка рисков для SIIL**. В частности, можно подготовить оценку стратегических и операционных, юридических, финансовых и репутационных рисков.

4. Шаг 4. Уведомление

Согласно законодательству Швейцарии, SIIL обязан как можно скорее сообщить о взломе данных специалисту Департамента по защите данных, если принято решение о необходимости его уведомления. **В указанный срок входят выходные дни и государственные праздники.**

Если принято решение не сообщать о взломе, специалист Департамента по защите данных должен сохранить краткую запись о происшествии с объяснением причины, по которой о происшествии не сообщалось.

Пострадавшие физические лица. Согласно статье 34 GDPR, когда она применима, SIIL обязан без излишнего промедления проинформировать пострадавших физических лиц, если взлом данных с большой вероятностью может стать серьезной угрозой для их конфиденциальности.

Если специалист Департамента по защите данных считает, что в результате взлома данных права и свободы физических лиц находятся под серьезной угрозой, следует без излишнего промедления сообщить пострадавшим физическим лицам о факте такого взлома данных.

В таких информационных сообщениях следует сообщить пострадавшим физическим лицам о мерах, которые они могут принять для снижения риска для

себя и отрицательных последствий, вызванных взломом данных. Специалист Департамента по защите данных должен определить наиболее приемлемые и действенные средства донесения информации о взломе данных до пострадавших физических лиц и при необходимости обратиться за содействием к консультантам по коммуникациям.

В уведомлениях следует четко указывать цель, чтобы пострадавшие физические лица могли принять надлежащие меры для своей защиты (например, заблокировать кредитную карту или изменить пароль) и чтобы дать регулирующим органам возможность выполнять свои функции, давать консультации и работать с претензиями. В каждом случае уведомление должно включать как минимум следующее:

- Описание характера взлома;
- Описание вероятных последствий взлома;
- Способ и время взлома;
- Пострадавшие данные;
- Описание мер по итогам взлома, принятых SIIL или предлагаемых ему; и
- Имя и контактные данные специалиста Департамента по защите данных и иных контактных лиц.

Прочие стороны. SIIL следует оценить, необходимо ли сообщить о происшествии каким-либо другим сторонам, и, при необходимости, обратиться за консультацией к ним (например, к компетентным органам, страховым компаниям, внешним юрисконсультантам и т.д.).

5. Шаг 5. Оценка и реагирование

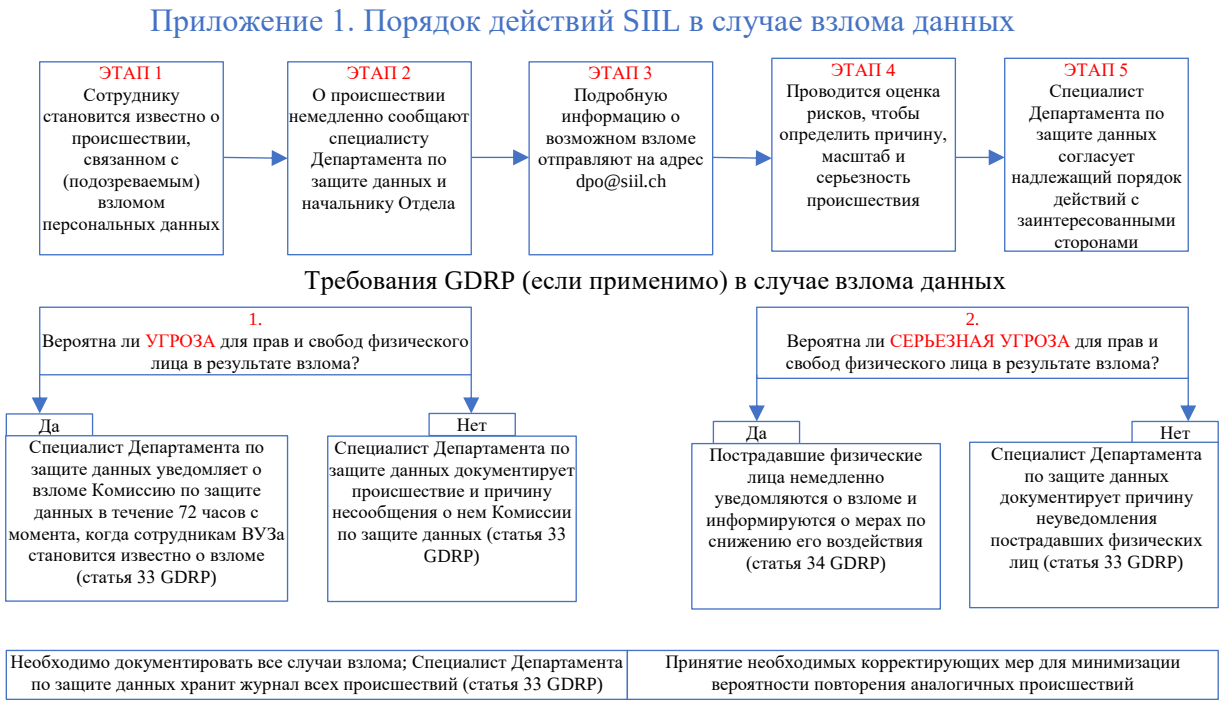
В некоторых случаях после первоначального расследования взлома данных необходимо дальнейшее подробное расследование, для которого может потребоваться содействие внешних провайдеров услуг по ИТ, юриспруденции и т.д., в зависимости от ситуации, чтобы установить весь масштаб взлома данных, его причины и вероятные последствия и принять действенные меры по его локализации. В течение этого периода отслеживаются последствия взлома данных и проводится повторная оценка. В таких случаях может потребоваться согласовать поэтапную программу уведомления со специалистом Департамента по защите данных.

После взлома данных необходимо провести анализ его последствий, чтобы убедиться в уместности и действенности мер, принятых во время происшествия, и определить сферы, которые в дальнейшем можно улучшить, например, актуализировать политики и процедуры или решить системные проблемы в случае их возникновения с целью снизить вероятность повторения аналогичных случаев взлома данных и обеспечить наличие надлежащих технических и организационных мер безопасности.

VI РАЗЪЯСНЕНИЯ

За дополнительной информацией и консультацией относительно порядка действий при подозрении на взлом данных следует обращаться к специалисту Департамента по защите данных в SIIL, Швейцария, по адресу электронной почты dpo@siil.ch.

VII ПРИЛОЖЕНИЕ 1. ПОРЯДОК ДЕЙСТВИЙ SIIL В СЛУЧАЕ ВЗЛОМА ДАННЫХ



Утверждено:	Академическим советом
Дата утверждения:	01.09.2022
Дата пересмотра:	01.09.2025
Ответственный:	Отдел ИТ
Контактное лицо:	p.tkachev@siil.ch