# Способы минимизации риска утечки конфиденциальной информации

**Малей Роман**
Главный специалист Управления внутреннего аудита ПАО «Юнипро» в областях: ИТ/ИБ аудиты, аудиты состояния безопасности и устойчивости бизнеса, цифровая аналитика, член Ассоциации «Институт внутренних аудиторов»[1]

**Статья предназначена для быстрого погружения в проблематику защиты конфиденциальной информации для лиц, не являющихся специалистами в области информационной безопасности. Сформирован необходимый теоретический минимум, предлагается подход «на языке управленца» к пониманию рисков нарушения защищенности информации и описывается вариативный конструктор для планирования и реализации практических мер по минимизации рисков утечки конфиденциальной информации.**

В условиях внешних вызовов устойчивость критических процессов в организациях и компаниях РФ становится актуальной и даже жизненно необходимой. Одним из важнейших аспектов сохранения конкурентоспособности, защищенности операционных процессов является обеспечение конфиденциальности[2] информации.

Информация пронизывает все существующие процессы, является главнейшим нематериальным активом. Угрозы нарушения конфиденциальности информации, особенно вероятность утечки и/или утраты конфиденциальной информации, формируют значимые операционные риски и требуют системного подхода по их минимизации. Как понять, что и где является конфиденциальной информацией в зоне ответственности?

Я предлагаю уважаемому читателю вместе со мной пройти все этапы от теории к практике и спроецировать взгляд на собственные имеющиеся или планируемые мероприятия.

Важно: статья не ставит целью научить подменять или изменять работу специалистов и экспертов в области ИБ. Без их непосредственного участия реализация всех описанных этапов не будет эффективной. В свою очередь, понимание их работы и способа мышления позволит получить синергический эффект и оптимизировать совместные усилия, а также контролировать мероприятия в части стратегических целей и задач организации.

## ЧТО ЗАЩИЩАТЬ?

В настоящее время существует большое количество законодательных актов, регуляторных и отраслевых требований и стандартов в области обеспечения информационной безопасности. Безусловно, должностные лица, ответственные в компании/организации за обеспечение информационной безопасности (далее — специалисты

1 Ассоциация «Институт внутренних аудиторов» (Ассоциация «ИВА»), зарегистрированная в 2000 г., является профессиональным объединением более чем 4000 внутренних аудиторов, внутренних контролеров и работников других контрольных подразделений российских компаний и организаций. Подробности на сайте www.iia-ru.ru.

2 Необходимость предотвращения разглашения, утечки какой-либо информации. В информационной безопасности придерживаются следующего определения: конфиденциальность информации — свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

ИБ), обязаны знать и применять на практике все требования и своевременно отслеживать изменения с корректировкой плана мероприятий.

Для операционных, функциональных и высших руководителей важно понимать, применительно к зоне ответственности процессов и процедур, имеющиеся виды информации, подлежащей защите от угроз, владеть актуальным перечнем угроз и потенциального ущерба процессам и деятельности компании от реализации таких угроз, уметь совместно со специалистами ИБ формировать и реализовывать приоритизированные меры по предотвращению угроз и восстановлению устойчивости процессов и деятельности, иметь инструменты эффективной системы контроля защищенности информации.

Специфика информации — в отличие от материальных активов, таких как финансовые или иные физически исчисляемые ресурсы, в случае утечки (утраты) защищаемой информации баланс или количество информационных активов не изменится. Прямые точки контроля на основе изменения количества (как в случае с утратой денежных ресурсов) не применимы. Требуется комплекс мероприятий, который на основе многофакторного анализа будет способен сигнализировать о признаках подготовки (предупреждение), реализации (предупреждение) или свершившемся факте утечки или утраты защищаемой информации (пресечение и профилактика).

**Виды защищаемой информации**:

- ПДн, персональные данные (факты, события и обстоятельства частной жизни гражданина, позволяющие идентифицировать его личность);
- ТС, тайна следствия и судопроизводства;
- СТ, служебная тайна (органов государственной власти);
- ПТ, профессиональная тайна (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);
- КТ, коммерческая тайна (сведения, связанные с коммерческой деятельностью, ноу-хау);
- КИИ, информация, обрабатываемая в значимых объектах[3] критической информационной инфраструктуры РФ.

**Хорошей практикой является составление реестра защищаемой информации (сведений конфиденциального характера), которая обрабатывается в зоне ответственности подразделения, блока, компании/ организации в целом, с указанием конкретных информационных систем и задействованных средств обмена (телекоммуникационные каналы связи, почтовые и нарочные отправление, электронный и физический документооборот), которые обрабатывают защищаемый вид информации или иным образом воздействуют на нее (системы управления, мониторинга, поддержания работоспособности и так далее).**

Защищаемую информацию целесообразно дополнительно разделить по фактору последствий нарушения конфиденциальности, то есть потенциального вида ущерба. Это не величина прямого или косвенного ущерба/убытка, который мы рассмотрим далее, а именно деление на соответствие требованиям (комплаенса) и непосредственно доходность компании/организации. Таким образом, **к комплаенсу относится ПДн, ТС, СТ, ПТ, КИИ по причине исключительно правовых,**

3 Объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры. Объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

**регуляторных и репутационных последствий от нарушения конфиденциальности указанных сведений, хотя и способных косвенно повлиять на устойчивость операционных процессов вследствие штрафных и ограничительных санкций.** В свою очередь, КТ является прямым активом компании или организации, который влияет на конкурентоспособность и устойчивость процессов и доходности деятельности в целом. Важно ответить на вопрос: компания/организация имеет цель реально защитить информацию или формально выполнить требования законодательства по ее защите?

## КАКИЕ РИСКИ МЫ ВИДИМ?

Специалисты ИБ применяют различные методы и подходы оценки рисков нарушения защищенности информации. В общем виде, защищают три основных состояния информации:

- **Конфиденциальность** (тема этой статьи).
- **Целостность**, то есть обеспечение достоверности и полноты информации и методов ее обработки.
- **Доступность**, то есть обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Данные состояния информации можно представить в виде равностороннего треугольника, в котором каждая вершина отвечает за максимальное значение состояния (обеспечено на 100%).

Точка внутри треугольника может указывать на планируемое и фактическое состояние защищенности конкретного вида информации в компании/организации. Исходя из приведенной парадигмы, невозможно добиться условий, которые обеспечат все состояния информации на 100%, — получается либо сбалансированная точка в центре треугольника, либо смещение к одной или двум вершинам, то есть приоритизация состояний защищенности. Данный парадокс можно представить следующей визуальной схемой (см. схему 2).

Схема 1. Треугольник состояний защищенности информации

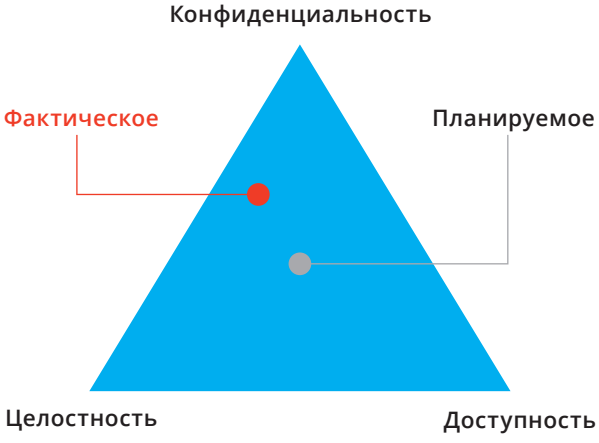


Схема 2. Совокупность состояний защищенности информации

**Угроза** информационной безопасности — это потенциальная возможность тем или иным способом нарушить состояние защищенности информации. Попытку реализации угрозы принято называть **атакой**. Лицо или событие, реализующее данную попытку, называется **злоумышленником** или **негативным событием**. Чаще всего угроза является следствием наличия уязвимых мест в объектах воздействия угрозы.

Виды угроз состояниям защищенности для простоты восприятия мы классифицируем по объектам воздействия угрозы на:

- **данные,** то есть информация и сведения в любом виде;
- **программы**, то есть информационные и автоматизированные системы, в которых обрабатываются данные;
- **аппаратуру,** то есть любое оборудование, на котором работают программы;
- **инфраструктуру,** то есть все поддерживающие элементы, такие как каналы связи, электроснабжение, системы безопасности, управляющие процессы.

По способу осуществления:

- случайные или преднамеренные;
- природного или техногенного характера.

По расположению источника:

- **внешние,** то есть злоумышленник или негативное событие воздействует с внешнего периметра компании/организации: криминальные элементы, промышленный шпионаж, хакерские атаки, халатные действия внешних партнеров и контрагентов, недобросовестные действия конкурентов;
- **внутренние,** то есть злоумышленник или негативное событие воздействует во внутреннем периметре: работники компании, партнеры, контрагенты и иные лица с доступом к информации, некорректные алгоритмы работы автоматизации и роботизации, чрезвычайные события внутреннего характера.

По носителю (источнику) конфиденциальной информации:

- люди (сотрудники, клиенты, посетители, обслуживающий персонал);
- документы материальные и в электронном виде;
- технические средства накопления и хранения информации, системы их обработки;
- выпускаемая продукция и/или услуги;
- производственные, промышленные отходы и т.д.

Существует различные методы оценки рисков операционных процессов в целом и информационной безопасности в частности. За редким исключением все они сводятся к оценке величины воздействия угрозы (ущерб) и потенциальной возможности реализации атаки (вероятность). Для простоты и лучшего восприятия предлагаю применять следующую формулу для конкретного вида защищаемой информации в реестре:

$$R_{ИБ} = (У_{угрозы} * В_{угрозы}),$$

$$\sum R_{ИБ} = (У_{угрозы\_1} * В_{угрозы\_1}) + ... + (У_{угрозы\_n} * В_{угрозы\_n}),$$

где

$R_{ИБ}$ — величина риска, в %;

$У_{угрозы}$ — величина потенциального ущерба, в %. Рассчитывается с учетом градаций по негативному воздействию на процесс/деятельность. Предлагается градация: ущерб минимальный (<5%), умеренный (от 6 до 15%), средний (от 16 до 30%), значительный (от 31 до 60%), аварийный (от 61 до 85%) и критический (от 86 до 100%);

$В_{угрозы}$ — величина вероятности реализации угрозы, в %. Расчет производится по априорному

(на основе знаний и прогнозирования) и/или апостериорному (на основе имеющегося опыта, ретроспективного анализа, всегда точнее и является основанием для повышения общего риска) определению вероятности наступления негативного события и величины прямого и косвенного ущерба для операционных процессов и деятельности в целом;

$\sum R_{ИБ}$ — суммарная величина риска, в %. Сумма всех имеющихся рисков конкретного вида защищаемой информации. Используется для сравнительного анализа и мониторинга.

Таким образом, основываясь на реестре защищаемой информации и результатах оценки рисков для каждого вида защищаемой информации в компании/организации, формируется карта рисков информационной безопасности.

**Пример**

*В компании «Автомобили и точка» имеются сведения о применяемых маркетинговых акциях и способах расчета и реализации бонусов для водителей и пассажиров, позволяющих удерживать лидирующие позиции в нише премиальных услуг такси в городе Примерово-Статейске. Сведения циркулируют в базах данных информационных систем, а также в серверных и пользовательских приложениях для сотрудников компании.*

*В приложении для пассажиров и водителей имеется возможность выбора акций для участия. Для сохранения устойчивости деятельности и высоких финансовых результатов необходимо обеспечить сохранность данных сведений (конфиденциальность) в тайне от потенциальных и действующих конкурентов и недобросовестных партнеров, при этом разумно гарантировать невозможность изменения условий и механизма акций без согласования со стороны руководства (целостность), в том числе обновлять для клиентского приложения список и условия акций и учитывать их при расчете бонусов (доступность).*

*С учетом имевшихся фактов утечки указанных сведений в прошлом году, приведших к критичному снижению прибыли и затрат на разработку новых маркетинговых акций, компания считает угрозу повторной утечки весьма вероятной и с очень высоким потенциальным ущербом. Данные сведения отнесены к коммерческой тайне, с высоким приоритетом к конфиденциальности (внешняя и внутренняя угроза) и умеренным приоритетом к целостности (внутренняя угроза, внешняя угроза в части клиентского фрода[4]) и доступности (внешняя и внутренняя угроза). Критический риск утечки конфиденциальной информации послужил причиной для разработки мер по предотвращению нарушений конфиденциальности сведений.*

## КАК МИНИМИЗИРОВАТЬ РИСКИ?

В зависимости от принятого в компании/организации аппетита[5] к рискам информационной безопасности необходимо разработать эффективный и реализуемый план мероприятий по минимизации недопустимых (превышающих порог толерантности) рисков. Например, для публичной, открытой компании/организации угроз конфиденциальности может просто не существовать — вся информация считается общедоступной. Однако нелегальный доступ представляется серьезной угрозой в случае комплаенс-требований (ПДн, КИИ и т.п.).

4 Действия клиентов, направленные на введение в заблуждение или использование уязвимостей действующих клиентских систем для подмены данных, в целях получения необоснованных привилегий, бонусов, скидок.

5 Общая величина риска, на который компания/организации готова пойти в условиях компромисса между риском и доходностью для получения одного или нескольких результатов.

На основе моделирования потенциальной атаки формируются варианты снижения вероятности реализации угрозы или устраняется негативная степень воздействия на процессы/деятельность путем реинжиниринга процессов, внедрения технических решений, организационных мер воздействия на потенциальных злоумышленников и события.

**Важно:** специалисты ИБ формируют модели злоумышленников и модели угроз в рамках реализации требований регуляторов и методик, стандартов обеспечения безопасности информации. Углубляться в данную тему в рамках статьи нецелесообразно, выделим только потенциальные каналы утечки конфиденциальной информации. Если же такие специалисты в компании/организации отсутствуют, настоятельно рекомендую воспользоваться услугами внешних консультантов или разовым договором ГПХ со специалистом ИБ, поскольку это очень трудоемкая и специфическая работа.

**Каналы утечки конфиденциальной информации операционные:**

- взаимодействие с контрагентами на основе договоров;
- запросы государственных органов, регуляторов;
- проведение переговоров с потенциальными контрагентами;
- посещения территории компании/организации;
- внешний и внутренний документооборот, особенно электронный;
- реклама, публикации в печати, интервью и т.п.

**Каналы утечки конфиденциальной информации технические:**

- естественный и искусственный акустический канал;
- визуальный канал;
- доступ к компьютерной сети;
- побочные электромагнитные излучения и наводки.

**Каналы утечки конфиденциальной информации человеческие:**

- через сотрудников компании (умысел, неосторожность, методы социальной инженерии и т.д.);
- через уволившихся или «обиженных» действующих сотрудников.

**Для снижения риска утечки или утраты конфиденциальной информации применимы следующие действенные меры:**

1. **Правовые** — создание режимов коммерческой тайны, патентов, авторских прав и т.д.
2. **Кадровые** — подбор, обучение, увольнение, контроль, план действий в нештатных ситуациях, изучение послужного списка и поведенческой модели ИТ-специалиста, иных пользователей с привилегированным доступом к информации и т.д.
3. **Конфиденциальное делопроизводство** — создание, хранение, уничтожение, передача документов и т.д.
4. **Режимные** — пропускной режим, внос и вынос документов, использование гаджетов на территории, удаленный доступ, охрана, доступ к информации и т.д.
5. **Организационные** — дробление конфиденциальной информации на части, дублирование на ключевых точках, использование систем хранения, резервное копирование, аудит и т.д.

6 **Инженерно-технические** — защита помещений, мест хранения информации, сигнализация, видеонаблюдение и т.д.

7 **Технические средства защиты информации** — DLP[6], шифрование, антивирусная защита, IDP/IDS[7], SEIM[8], правильная настройка оборудования, защищенное программное обеспечение и т.д.

**Важно:** для рисков, связанных с внутренними каналами утечки конфиденциальной информации, основанных на человеческом факторе, рекомендую придерживаться следующей парадигмы — весь персонал априори можно разделить на три условные группы поведенческой модели:

**1 группа — «хулиганы»:** нарушители установленных норм и правил, невзирая на существующие организационные и правовые ограничения и требования, с прямым или косвенным умыслом. Составляют около 15% от общего количества персонала. Компенсирующие меры: технический запрет на несанкционированные действия, документирование всех действий в информационной среде работодателя, проверка и отбор при устройстве на работу на основании сведений от предыдущих работодателей и поведенческих установок.

**2 группа — «законопослушные»:** полностью исполняют все требования, нормы и правила. Составляют около 20% от общего количества персонала. Возможны риски, связанные с действиями по халатности без умысла (попытка угодить всем правилам, ошибка «отличника»). Компенсирующие меры: технический запрет на несанкционированные действия, обучение и тренинги в области информационной безопасности.

**3 группа — «приспособленцы»:** нарушают действующие нормы и правила в зависимости от выстроенной вокруг них системы возможностей. При отсутствии понимания ответственности за действия или бездействие и технической возможности — будут принимать решения о нарушении требований, норм и правил в зависимости от личной выгоды от таких действий. Составляют более 65% от общего количества персонала. Являются источником (носителем) каналов утечки информации по соучастию/содействию с внешними злоумышленниками. Компенсирующие меры: технический запрет на несанкционированные действия, информирование о тяжести последствий за действия/бездействие, в случае подозрения на подготовку к реализации угрозы — документирование всех действий в информационной среде работодателя. Основная группа, на которую направлены меры по минимизации рисков.

**Пример**

*В компании «Автомобили и точка», руководствуясь моделями нарушителя и моделями угроз, определили наиболее вероятные каналы утечки конфиденциальной информации, связанной со сведениями о применяемых маркетинговых акциях и способах расчета и реализации бонусов для водителей и пассажиров. Определен круг лиц (внутренних работников и партнеров, а также внешних лиц с потенциальным доступом). К ним отнесены сотрудники департамента ИТ, маркетинга, анализа данных,*

6 Data Leak Prevention — системы, которые предупреждают утечки данных на основе анализа исходящего сетевого трафика.

7 Intrusion Detection System — система обнаружения вторжений. Intrusion Prevention System — система предотвращения вторжений.

8 Security information and event management — объединение двух терминов, обозначающих область применения. SIM (Security information management) — управление информацией о безопасности, SEM (Security event management) — управление событиями безопасности.

*клиентского сервиса, контрагенты по рекламной продукции, разработчики и техническая поддержка клиентского приложения на удаленном доступе. С учетом изучения кадровой службой указанных работников определена их относимость к одной из трех групп поведенческой модели. Сформированы предложения и защищен бюджет по внедрению технических средств документирования действия работников и иных лиц в информационном пространстве (программно-аппаратные агенты Task mining[9] на локальных и удаленных рабочих местах и в системах), средства предотвращения утечки информации DLP, системы обнаружения и предотвращения атак IDS/IPS.*

*Введен режим коммерческой тайны, документы и информация помечаются ограничительной меткой — грифом КТ. Выделен участок конфиденциального документооборота. Разработаны и проводятся дополнительные тренинги и информационные рассылки о важности и ответственности за соблюдение требований режима коммерческой тайны.*

*Проведен стресс-тест устойчивости системы начисления бонусов на выделенном виртуальном сервере, максимально приближенном по действиям и нагрузке к реальной среде за счет роботизированных операций. В настоящее время реализованных (завершенных до факта утечки, утраты) атак на конфиденциальность информации в компании не зафиксировано.*

## РЕЗЮМЕ

Общими принципами выстраивания эффективной стратегии минимизации рисков утечки конфиденциальной информации являются:

1. **Системный подход** — от отбора и обучения персонала до создания регламентов работы, связанных с обработкой конфиденциальной информации, идентификации личности посетителей. Более высокий уровень зрелости ИБ — регламентация работы с компьютерами, сетью и технологиями.

2. **Вариативность** — никогда не поддавайтесь чувству полной защищенности. Не доверяйте полностью конфиденциальную информацию чему-либо — носителям, шифрам, хранилищам. Ваша информация может быть получена третьими лицами независимо от принятых мер. Всегда старайтесь формировать конфиденциальную информацию в таком виде, чтобы непосвященному человеку было труднее разобраться в данных. Подозревайте всех, не верьте в безграничные возможности новых технологий. Можно спровоцировать управляемую утечку неактуальной конфиденциальной информации, проследить за процессом и выявить злоумышленника.

3. **Достаточность** — кроме руководителя, не должно быть человека, владеющего всей полнотой информации по зоне его ответственности. Поэтому злоумышленнику придется собирать ее из разных источников и носителей, что снижает вероятность реализации угрозы.

4. **Дробление** — храните конфиденциальную информацию и пересылайте ее по разным каналам. Никогда не посылайте вместе логин и пароль. Если отправляете пароль по защищенной корпоративной почте, направьте логин по смс или назовите его по телефону.

9 Технология, направленная на отслеживание, фиксацию и аналитику всех действий, которые осуществляет лицо на автоматизированном рабочем месте.