Риски CEO, CIO, CISO при нарушении требований 143 ФЗ, 152 ФЗ, 187 ФЗ, 250 указа Президента, 21 приказа ФСТЭК и других нормативных документов.

V 1.2

Преамбула

Настоящий документ представляет собой методологическую основу для должностных лиц, ответственных за безопасность информации, с целью:

1. Структурированного понимания персональной ответственности, устанавливаемой законодательством РФ для должностных лиц субъектов КИИ и операторов персональных данных (УЗ-3 и выше).
2. Формирования практического подхода к управлению личными профессиональными рисками, связанными с исполнением обязанностей в области защиты информации.

Особенностью российского законодательства является перекос ответственности за несоблюдение требований защиты информации в область персональной ответственности должностных лиц, что приводит к дисбалансу прав и ответственности, поскольку решения о финансировании соответствия систем защиты принимается организацией, а ответственность за фактическое несоответствие несут должностные лица вплоть до тюремного заключения.

Целевой аудиторией документа являются:

- Должностные лица, несущие персональную ответственность за обеспечение безопасности информации: руководители организаций (CEO), руководители и специалисты служб информационной безопасности (CISO), руководители IT-подразделений (CIO).
- Кандидаты на соответствующие должности.
- Организации, отнесенные к субъектам критической информационной инфраструктуры (КИИ), а также операторы персональных данных, обрабатывающие данные в объеме, отнесенном к уровню защищенности УЗ-3 и выше согласно постановлению Правительства РФ от 01.11.2012 № 1119.

Данный документ может служить отправной точкой для самооценки должностным лицом своей роли и зоны персональной ответственности, разграничения внутреннего разграничения полномочий между CEO, CISO и CIO, а также инициации и разработки конкретных внутренних процедур и регламентов, направленных на снижение персональных юридических и профессиональных рисков.

Структура ответственности по сценариям:

Тексты статей кодексов приведены в конце документа

1. Сценарий 1. Нарушения в области защиты информации были выявлены до возникновения инцидента в области информационной безопасности.
    a. Если прокуратура или РКН нашли несоответствие мер защиты ОКИИ или ПД требованиям, то ответственный или причастный к ИБ рискует быть наказан по
        i. КоАП ч. 8 ст. 13.11 до 200 000 р.
        ii. КоАП ч. 1 ст. 13.12 до 50 000 р.

iii. УК ст. 293 до 120 000р, до 3-х годовых зарплат, до 3 месяцев ареста.

b. Если проверка выявила занижение категории КИИ, исключение АСУ из категорирования, занижении категории ПД, то ответственный или причастный может быть наказан по
   i. УК ст. 292 до 500 000 р., до 4-х лет.

2. Сценарий 2. Нарушения были выявлены следствием в процессе расследования инцидента в области информационной безопасности.
   a. Воздействие на ОКИИ, о котором вы обязаны сообщить и следствие выявило нарушения, то ответственный и причастные могут быть привлечены по
      i. КоАП ч.14 ст. 13.11 до 600 000 р.
      ii. УК ч. 3 ст. 274.1 от 3 до 8 лет лишения свободы.
      iii. УК ст. 293 до 120 000р, до 3-х годовых зарплат, до 3 месяцев ареста.
   b. Утечка персональных данных от 100 тыс.
      i. УК ч. 3 ст. 274.1 от 3 до 8 лет лишения свободы.
      ii. УК ст. 293 до 120 000р, до 3-х годовых зарплат, до 3 месяцев ареста.

Основные заблуждения относительно правоприменительной практики:

1. Сейчас мало приговоров по этим статьям.
   a. Верно. Однако наблюдается устойчивая экспоненциальная динамика роста количества возбужденных дел и вынесенных судебных решений, что свидетельствует об активизации правоприменительной практики.
2. Умысел нужно доказать.
   a. Правоприменитель выработал устоявшиеся и принимаемые судами формулировки мотивов, подпадающих под признаки «корыстной или иной личной заинтересованности» (ст. 201 УК РФ) или «иных низменных побуждений». К таковым относятся, в частности:
      i. «из чувства ложно понятого служебного долга, солидарности с [ФИО], карьеризма и желания выслужиться перед руководителем» (приговор от 17.03.2020 № 1-286/2020);
      ii. «преследуя личную заинтересованность, выраженную в карьеризме, желании предотвратить негативную оценку своих профессиональных качеств со стороны руководства» (приговор от 16.05.2022 № 1-182/2022).
3. Тяжелые части статей не применимы.
   a. Не верно. Наличие между обвиняемым и работодателем трудовых отношений (трудового договора) и закрепленных в должностной инструкции полномочий по обращению с информацией следственные органы и суды квалифицируют как использование служебного положения. Данный признак является основанием для применения более строгих санкций, предусмотренных частями 2 и 3 соответствующих статей Уголовного кодекса Российской Федерации.

Наиболее часто встречающиеся грубые ошибки при спасении фигурантов.

1. Взаимодействие со следствием для смягчения наказания.

Активное сотрудничество с органами предварительного следствия, формально являющееся смягчающим обстоятельством, сопряжено с существенным процессуальным риском. Предоставление информации и доказательств может быть использовано для переквалификации деяния на более тяжкий состав статьи или для установления вины иных лиц. В связи с этим стратегия защиты должна исключать добровольное свидетельствование против себя по уголовному составу в расчете на смягчение административной ответственности, так как данная тактика является процессуально несостоятельной и ведет к ухудшению правового положения. Все контакты со следственными органами должны осуществляться исключительно через адвоката, специализирующегося на делах в сфере информационной безопасности.

2. Отсутствие документированных свидетельств информирования организации о несоответствиях.

Устные доклады первому лицу или иным руководителям о выявленных нарушениях в защите персональных данных или объектов КИИ не создают юридически значимого подтверждения осведомленности организации. Отсутствие письменного запроса на ресурсы для устранения нарушений лишает должностное лицо возможности доказать, что руководство было уведомлено, но не выделило необходимых средств. Единственным надлежащим способом фиксации является направление официальных служебных записок с обязательной регистрацией в службе делопроизводства. В таких документах должны быть четко указаны конкретные нарушения и перечень необходимых мер для приведения состояния защиты в соответствие с законодательством РФ.

3. Отсутствие планов устранения явных и легко выявляемых нарушений.

При выявлении явных нарушений в ходе проверки уполномоченных органов отсутствие формализованного плана по их устранению трактуется как бездействие и отсутствие намерения соблюдать закон. Наличие внутренне утвержденного и визированного «Плана мероприятий по устранению выявленных недостатков» является ключевым доказательством добросовестности организации. Данный документ служит основанием для конструктивного диалога с проверяющими органами, демонстрируя осознание проблем и курс на их планомерное исправление, что может позитивно влиять на вид и меру применяемой ответственности.

4. Использование иностранных средств защиты информации.

Применение иностранного программного обеспечения и оборудования для защиты информации в ряде случаев прямо запрещено нормативными актами, в частности Указом Президента РФ № 250. Нарушение данного запрета при обработке информации ограниченного доступа или в инфраструктуре КИИ создает непреодолимые правовые риски и может являться самостоятельным составом нарушения. Перед внедрением любых средств защиты необходимо проводить анализ их соответствия действующим ограничениям, установленным указами Президента РФ и постановлениями Правительства РФ.

5. Почивания на лаврах успешных проектов по информационной безопасности.

Субъективная уверенность должностных лиц в полноте выполненных мероприятий по защите информации не имеет доказательственной ценности. Рекомендуемым механизмом получения объективной оценки является проведение регулярного независимого аудита системы защиты информации аккредитованной организацией.

Результаты такого аудита носят конфиденциальный характер и предназначены исключительно для внутреннего использования с целью совершенствования системы защиты. Предоставление отчета об аудите третьим лицам, включая контролирующие органы, должно осуществляться только при наличии прямого законного требования, поскольку данный документ может содержать информацию, способную спровоцировать внеплановую проверку.

Административная ответственность

КоАП РФ Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных

8. **Невыполнение оператором при сборе персональных данных**, в том числе посредством информационно-телекоммуникационной сети "Интернет", **предусмотренной законодательством Российской Федерации в области персональных данных обязанности** <…>

<…>; **на должностных лиц - от ста тысяч до двухсот тысяч рублей**; **на юридических лиц - от одного миллиона до шести миллионов рублей**.

14. **Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации**, включающей персональные **данные более ста тысяч субъектов персональных данных** <..>

<…> **на должностных лиц - от четырехсот тысяч до шестисот тысяч рублей**; **на юридических лиц - от десяти миллионов до пятнадцати миллионов рублей**.

КоАП РФ Статья 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

1. **Нарушение требований** к **созданию** систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и **обеспечению их функционирования** либо требований по **обеспечению безопасност**и значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие действия (бездействие) не содержат признаков уголовно наказуемого деяния, -

влечет наложение административного штрафа на должностных лиц в размере **от десяти тысяч до пятидесяти тысяч рублей**; на юридических лиц - от пятидесяти тысяч до ста тысяч рублей.

Уголовная ответственность:

УК РФ Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

<…>

3. **Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации** <…> если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, -

наказывается <…>

4. **Деяния, предусмотренные частью** первой, второй или **третьей** настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом **с использованием своего служебного положения**, -

наказываются **лишением свободы на срок от трех до восьми** лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

УК РФ Статья 293. Халатность

1. **Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей** вследствие недобросовестного или небрежного отношения к службе либо обязанностей по должности, если это повлекло причинение крупного ущерба или **существенное нарушение прав** и законных интересов граждан или организаций либо охраняемых законом **интересов общества или государства**, -

наказывается **штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до трех месяцев**.

УК РФ Статья 292. Служебный подлог

1. Служебный подлог, то есть внесение должностным лицом, <…>, в официальные документы заведомо ложных сведений, а равно внесение в указанные документы исправлений, искажающих их действительное содержание <…> -

<…>.

2. **Те же деяния, повлекшие существенное нарушение** прав и законных интересов граждан или организаций либо охраняемых законом **интересов общества или государства**, -

наказываются

- штрафом в размере **от ста тысяч до пятисот тысяч рублей** или
- в размере заработной платы или иного дохода осужденного за период от одного года до трех лет,
- либо **принудительными работами на срок до четырех лет** с лишением права занимать определенные должности или
- заниматься определенной деятельностью на срок до трех лет или без такового, либо
- **лишением свободы на срок до четырех лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Дата	Место
21/11/2025	г. Москва

Каранкевич Максим Андреевич

https://levelmax.pro
me@levelmax.pro
+7 905 205 15 55