ЗАО «РИТЭЙЛ КОНСАЛТ» (участник холдинга «5 ЭЛЕМЕНТ)
пр-т Дзержинского, 8, пом. 306
220036, г. Минск, Республика Беларусь, УНП 192244151
sales@cyber5.by, +375292178825, +375339903840

Техническая и криптографическая защита информации
(в том числе аттестация системы защиты информации)

В соответствии с Законом Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» информация, распространение и (или) предоставление которой ограничено (в том числе персональные данные, охраняемая законом тайна), должна обрабатываться в информационных системах с применением **системы защиты информации**, аттестованной в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь.

При этом для создания системы защиты информации используются исключительно средства технической и криптографической защиты информации (межсетевые экраны, антивирусное программное обеспечение, система обнаружения вторжений, система предотвращения вторжений, средства шифрования, SIEM-системы и т.п.), **имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, порядок проведения которой определяется Оперативно-аналитическим центром при Президенте Республики Беларусь**.

Согласно статьи 17 Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» **одной из обязательных мер по обеспечению защиты персональных данных является осуществление технической и криптографической защиты персональных данных** в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

Порядок осуществления технической и криптографической защиты определен Оперативно-аналитическим центром в приказе от 20.02.2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449».

Работы по технической и криптографической защите включают:

проектирование системы защиты информации;

создание системы защиты информации;

аттестацию системы защиты информации в соответствии с Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным приказом, утверждающим настоящее Положение;

обеспечение функционирования системы защиты информации в процессе эксплуатации информационной системы;

обеспечение защиты информации в случае прекращения эксплуатации информационной системы.

При этом персональная ответственность за организацию работ по технической и криптографической защите информации в организации, обеспечение кибербезопасности организации возложена на ее руководителя (пункт 15 Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации», подпункт 3.15 пункта 3 Указа Президента Республики Беларусь от 14.02.2023 № 40 «О кибербезопасности»).

Ответственность:

Статьей 203-2 Уголовного кодекса Республики Беларусь установлена ответственность за несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим обработку

персональных данных, повлекшее по неосторожности их распространение и причинение тяжких последствий.

Статья 203-2. Несоблюдение мер обеспечения защиты персональных данных

Несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим обработку персональных данных, повлекшее по неосторожности их распространение и причинение тяжких последствий, -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до одного года, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на срок до одного года.

За исключением указанного, Уголовный кодекс (УК) не содержит специальных составов, предусматривающих ответственность за нарушения законодательства в сферах обеспечения кибербезопасности, технической и криптографической защиты (ТКЗИ).

В этой связи к группе уголовно наказуемых противоправных деяний, выражающихся в формировании причин и условий, способствующих совершению преступлений, объектом посягательств которых выступают общественные отношения, связанные с безопасным функционированием информационной системы организации, относятся преступления против интересов службы (глава 35 УК):

бездействие должностного лица (статья 425 УК);

служебная халатность (статья 428 УК) и др., совершенные должностным лицом (руководителем) организации, на которого возложена персональная ответственность за организацию работ по ТКЗИ, а также обеспечение кибербезопасности возглавляемой организации.

Ответственность руководителя обусловлена его ролью в принятии управленческих решений, связанных, прежде всего, с финансированием работ по ТКЗИ, обеспечению кибербезопасности.

Статьей 23.7 КоАП предусмотрена административная ответственность за нарушение законодательства о персональных данных:

Статья 23.7. Нарушение законодательства о защите персональных данных

1. Умышленные незаконные сбор, обработка, хранение или предоставление персональных данных физического лица либо нарушение его прав, связанных с обработкой персональных данных, -

влекут наложение штрафа в размере до пятидесяти базовых величин.

2. Деяния, предусмотренные частью 1 настоящей статьи, совершенные лицом, которому персональные данные известны в связи с его профессиональной или служебной деятельностью, -

влекут наложение штрафа в размере от четырех до ста базовых величин.

3. Умышленное незаконное распространение персональных данных физических лиц -

влечет наложение штрафа в размере до двухсот базовых величин.

4. ***Несоблюдение мер обеспечения защиты персональных данных физических лиц -***

влечет наложение штрафа в размере от двух до десяти базовых величин, на индивидуального предпринимателя - от десяти до двадцати пяти базовых величин, ***а на юридическое лицо - от двадцати до пятидесяти базовых величин.***

Осуществление технической и криптографической защиты – обязательная мера обеспечения защиты персональных данных.

Более того, в 2026 году Кодекс об административных правонарушениях дополнен статьями 23.11, 23.12, закрепляющими административную ответственность за нарушение требований по кибербезопасности:

Статья 23.11. Нарушение требований по кибербезопасности

1. Невыполнение или ненадлежащее выполнение собственником (владельцем) объекта информационной инфраструктуры, эксплуатация которого возможна без применения системы защиты

информации, требований по кибербезопасности, повлекшее возникновение киберинцидента высокого уровня, –

влечет наложение штрафа в размере от десяти до двадцати базовых величин, а на юридическое лицо – от двадцати до ста базовых величин.

2. Невыполнение или ненадлежащее выполнение собственником (владельцем) информационной системы, эксплуатация которой осуществляется с применением системы защиты информации, требований законодательства по технической и криптографической защите информации, повлекшее возникновение киберинцидента высокого уровня, –

влечет наложение штрафа в размере от десяти до двадцати пяти базовых величин, а на юридическое лицо – ***от двадцати пяти до ста двадцати пяти базовых величин.***

3. Эксплуатация информационной системы без применения системы защиты информации, когда обязанность такого применения предусмотрена законодательными актами, повлекшая возникновение киберинцидента высокого уровня, –

влечет наложение штрафа в размере от пятнадцати до пятидесяти базовых величин, а на индивидуального предпринимателя или юридическое лицо – ***от сорока до двухсот базовых величин.***

4. Невыполнение или ненадлежащее выполнение центром обеспечения кибербезопасности и реагирования на киберинциденты предъявляемых к таким центрам требований, повлекшее наступление киберинцидента высокого уровня на объекте информационной инфраструктуры организации, которой такой центр оказывает услуги по обеспечению кибербезопасности, –

влечет наложение штрафа в размере от десяти до ста пятидесяти базовых величин, а на юридическое лицо – от двадцати до шестисот базовых величин.

Статья 23.12. Нарушение требований по кибербезопасности критически важных объектов информатизации

1. Невыполнение или ненадлежащее выполнение владельцем критически важного объекта информатизации требований по технической и криптографической защите информации, повлекшие возникновение киберинцидента высокого уровня на критически важном объекте информатизации, -

влекут наложение штрафа в размере от двадцати пяти до пятидесяти базовых величин, а на юридическое лицо - от пятидесяти до двухсот пятидесяти базовых величин.

2. Те же деяния, повлекшие причинение ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах, -

влекут наложение штрафа в размере от пятидесяти до ста базовых величин, а на юридическое лицо - от ста до пятисот базовых величин.

3. Невыполнение владельцем объекта информатизации требований законодательства по отнесению такого объекта к критически важному и обеспечению технической и криптографической защиты обрабатываемой на нем информации, повлекшее возникновение киберинцидента высокого уровня на данном объекте информатизации, -

влечет наложение штрафа в размере от семидесяти пяти до ста пятидесяти базовых величин, а на юридическое лицо - от ста пятидесяти до семисот пятидесяти базовых величин.

4. То же деяние, повлекшее причинение ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах, -

влечет наложение штрафа в размере от ста до двухсот базовых величин, а на юридическое лицо - от двухсот до тысячи базовых величин.

Помимо указанного невыполнение требований по технической и криптографической защите может повлечь **приостановление обработки персональных данных в информационных ресурсах компании** (сайт, мобильное приложение, CRM, иные ресурсы).

Согласно пункту 23 Положения о Национальном центре защиты персональных данных, утвержденного Указом Президента Республики Беларусь от 28.10.2021 № 422 «О мерах по совершенствованию защиты персональных данных», в случае выявления по результатам плановой или внеплановой проверки нарушений законодательства о персональных данных, отраженных в акте плановой или внеплановой проверки, **директор Национального центра защиты персональных данных в течение 10 рабочих дней со дня окончания проверки выносит письменное требование (предписание) об устранении выявленных нарушений и (или) приостановлении (прекращении) обработки персональных данных в информационном ресурсе (системе)** с указанием конкретных действий, которые должны быть приостановлены

(прекращены), и устанавливает срок такого устранения и (или) приостановления (прекращения), не превышающий шести месяцев.

Важно помнить про практическую кибербезопасность организации:

Последствия кибератаки злоумышленников:
39% – шифрование данных
17% – утечка персональных данных
11% – закрепление для продолжения атаки

Индустрии, подверженные кибератакам:
19% – государственные учреждения
17% – промышленность
15% – IT
11% – финансовые организации

Способы проникновения хакеров в инфраструктуру компаний:
44% – уязвимости в публичных приложениях
25% – скомпрометированные учетные данные
16% – атаки через IT-подрядчиков.

Цель злоумышленника – блокирование продуктивной деятельности организации посредством шифрования баз данных, блокирования АСУТП, кражи персональных данных с последующим вымогательством денежных средств.

ЗАО «РИТЭЙЛ КОНСАЛТ» (входит в состав холдинга «5 ЭЛЕМЕНТ») имеет специальное разрешение (лицензию) Оперативно-аналитического центра при Президенте Республики Беларусь (номер лицензии в Едином реестре лицензий: 22250000081853) на деятельность по технической и криптографической защите информации и выполняет полный перечень работ по технической и криптографической защите информации:

проектирование систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;

создание систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, в том числе внедрение средств защиты информации, проверка их работоспособности и совместимости с активами информационной системы;

аттестация систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

ЗАО «РИТЭЙЛ КОНСАЛТ» оказывает широкий спектр услуг в области кибербезопасности, в том числе:

обследование (аудит) систем защиты информации информационных систем, в том числе технических, программных средств обработки информации, на соответствие требованиям законодательства;

реализация и внедрение средств защиты информации;

автоматизированная инвентаризация активов;

администрирование средств защиты информации;

технический анализ защищенности (пентест);

анализ исходного кода на уязвимости.

В состав холдинга «5 ЭЛЕМЕНТ» входит аттестованный Оперативно-аналитическим центром при Президенте Республики Беларусь Центр обеспечения кибербезопасности и реагирования на киберинциденты (далее – ЦКБ «5 ЭЛЕМЕНТ»).

ЦКБ «5 ЭЛЕМЕНТ» оказывает услуги по обеспечению кибербезопасности:

круглосуточный мониторинг кибербезопасности объектов информационной инфраструктуру организаций-заказчиков;

выявление киберинцидентов и реагирование на киберинциденты на объектах информационной инфраструктуры организаций-заказчиков;

расследование киберинцидентов на объектах информационной инфраструктуры организаций-заказчиков, анализ информации о киберинцидентах и кибератаках, установление причин киберинцидентов;

ликвидация последствий киберинцидентов;

анализ защищенности объектов информационной инфраструктуры.

По вопросам сотрудничества предлагаем обращаться к заместителю директора Гречаникову Максиму по телефону +37529 217 88 25 или по адресу электронной почты maxim.grechanikov@cyber5.by, отдел продаж по телефону +37533 990 38 40 или адресу электронной почты sales@cyber5.by.