K2 кибер безопасность

ANTI-MALWARE

ИССЛЕДОВАНИЕ ГОТОВНОСТИ СУБЪЕКТОВ КИИ К ИСПОЛНЕНИЮ ЗАКОНОДАТЕЛЬСТВА (187-ФЗ)

ОГЛАВЛЕНИЕ

Исследование готовности субъектов КИИ к исполнению законодательства (187-ФЗ)

Введение и методология

Федеральный закон о безопасности критической информационной инфраструктуры был принят шесть лет назад, и несмотря на это вопрос защиты КИИ остается актуальным, особенно последние два года, когда наблюдается рекордный всплеск кибератак во всех отраслях. Сроки и ответственность, зафиксированные в указах 2022 года, заставляют бизнес и госструктуры сфокусироваться на как можно более оперативной реализации аудита инфраструктуры и бизнес-процессов и организации их защиты.

Мы решили составить целостную картину происходящего в области защиты КИИ – выяснить, как компании реагируют на изменения, насколько далеки они от поставленных целей и хватит ли вендорам и поставщикам услуг возможностей и компетенций, чтобы удовлетворить спрос и требования рынка. Для этого был проведен опрос представителей бизнеса — ИТ- и ИБ-директоров, а также представителей вендоров, ответственных за разработку и продвижение продуктов в области информационной безопасности.

Аудитория

ИТ- и ИБ-руководители крупных российских компаний и госкорпораций, 62% опрошенных (61 компания) – с выручкой более 5 млрд руб., в отраслях:

- электроэнергетика
- металлообработка
- медицина и фармацевтика
- металлургия
- транспорт и логистика
- горная добыча
- химическая промышленность
- финансы
- нефтегазовая промышленность

Представители компаний, которые занимаются разработкой аппаратного и программного обеспечения для информационной безопасности или оказывают услуги обследования инфраструктуры и категорирования объектов.

Выборка

108
респондентов

Период

июнь-август 2023 г.

Методология

глубинные интервью с последующей нормализацией для статистического анализа

K2 кибер безопасность

ANTI-MALWARE

Ключевые выводы

Подавляющее число компаний приступили к выполнению требований ФЗ, при этом каждая десятая компания только готовится к запуску работ. Основные препятствия — сложность понимания ФЗ и внутренние трудности с выстраиванием организационных процессов.

Среди компаний, которые уже приступили к работам

8%

полностью завершили проекты по созданию СОИБ, удовлетворяющей требованиям 187-ФЗ

77%

находятся на старте этой деятельности

Но далеко не все уверены в обоснованности затрат на защиту КИИ в соответствии с законодательством.

52%

считают, что требования 187-ФЗ соответствуют реальным угрозам.

Большинство компаний скептически относятся к возможности реализации проектов защиты КИИ на базе отечественных решений.

48%

опрошенных уверены в том, что российские продукты справятся с требованиями закона

31%

категорически не удовлетворены тем, что предлагает рынок

Проекты создания СОИБ связаны с серьезными трудностями для большинства организаций.

29%

опрошенных сообщили, что не столкнулись с проблемами на различных этапах реализации

187-ФЗ и сжатые сроки его обязательного исполнения вынуждают компании увеличивать расходы на безопасность.

22%

компаний остаются в рамках своих бюджетов на ИБ.

61%

опрошенных полностью уверены, что уложатся в указанный срок

12%

признаются в том, что скорее всего его нарушат

Для российских вендоров вступление в действие 187-ФЗ в 2018 году стало драйвером роста, так как простимулировало спрос на их решения. Компании развивают свои продукты, обогащают их новыми технологиями, разрабатывают дополнительные решения для автоматизации организационных задач, активно проходят сертификацию оборудования и ПО.

01

СФЕРА ДЕЙСТВИЯ И ОСНОВНЫЕ ПОНЯТИЯ 187-ФЗ

Сфера действия и основные понятия 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

1 января 2018 года вступил в действие Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1] (далее 187-ФЗ). 187-ФЗ регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры РФ (далее – КИИ) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

В 187-ФЗ установлены следующие определения:

- критическая информационная инфраструктура – объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов;
- объекты КИИ – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ (далее – ИС, ИТС, АСУ).

К субъектам КИИ относятся государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТС, АСУ, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, в банковской сфере и иных сферах финансового рынка, топливно-энергетическом комплексе, в атомной энергетике, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности; российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Для того чтобы понять, является ли организация субъектом КИИ, необходимо проанализировать следующие документы:

- устав организации;
- выписка из ЕГРЮЛ, содержащая коды ОКВЭД;
- лицензии, сертификаты;
- иные положения и разрешительные документы, где прописаны основные и вспомогательные виды деятельности;
- проектная документация на ИС, ИТС, АСУ, принадлежащие организации на законном основании (ТЗ, паспорт и т.д.).

Если организация попадает под действие 187-ФЗ: с чего начать

После того как было определено, что организация является субъектом КИИ, необходимо провести категорирование объектов КИИ в соответствии с Постановлением Правительства №127[2].

Для этого нужно:

1. Создать комиссию по категорированию объектов КИИ (далее – Комиссия), которая в ходе своей работы:
    1. определяет, какие процессы реализует организация для выполнения функций или осуществления видов деятельности;
    2. выявляет процессы, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее – критические процессы);
    3. формирует перечень объектов КИИ: перечень ИС/АСУ/ИТС, которые используются для реализации каждого критического процесса.

2. Перечень объектов КИИ направляется на согласование в государственный орган или российское юридическое лицо, выполняющее функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере в части подведомственных им субъектов КИИ (в головную организацию при ее наличии). Согласованный и утвержденный перечень направляется в течение 10 рабочих дней на согласование во ФСТЭК России.

3. Комиссия в течение одного года должна провести категорирование объектов КИИ. Постановлением Правительства №127 установлено 3 категории значимости объектов КИИ. Для того чтобы определить категорию объекта, Комиссия:
    1. рассматривает возможные действия нарушителей и анализирует угрозы безопасности информации в отношении объектов КИИ;
    2. оценивает в соответствии с перечнем показателей критериев значимости масштаб последствий в случае возникновения компьютерных инцидентов на объектах КИИ, определяет значения каждого показателя или обосновывает их неприменимость;
    3. устанавливает каждому из объектов КИИ одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости;
    4. оформляет акт категорирования.

4. В течение 10 рабочих дней после утверждения акта категорирования во ФСТЭК России для согласования направляются сведения о результатах присвоения объектам КИИ категории значимости либо об отсутствии необходимости присвоения одной из таких категорий. Сведения оформляются в соответствии с формой, приведенной в Приказе ФСТЭК от 22.12.2017 № 236[3].

5. ФСТЭК России проверяет предоставленные сведения в течение 30 дней со дня получения. Если порядок категорирования соблюден, и категория присвоена верно, ФСТЭК России вносит сведения об объекте КИИ в реестр значимых объектов и уведомляет об этом субъекта. Если выявлены нарушения, предоставленные сведения возвращаются субъекту в течение 10 дней с момента поступления с обоснованием причин. Субъект должен в течение 10 дней устранить замечания и отправить сведения повторно.

6. Субъект КИИ не реже одного раза в 5 лет, а также в случае изменения показателей критериев значимости объектов КИИ или их значений осуществляет пересмотр результатов категорирования принадлежащих ему объектов КИИ.

Дальнейшие шаги по выполнению требований 187-ФЗ и обеспечению безопасности объектов КИИ

После категорирования объектов КИИ субъект должен разработать и осуществить мероприятия по обеспечению безопасности значимых объектов КИИ (далее – ЗОКИИ) в соответствии с Приказом ФСТЭК России от 21.12.2017 № 235[4] и Приказом ФСТЭК России от 25.12.2017 № 239[5].

Мероприятия включают в себя:

1. Создание системы безопасности, обеспечивающей устойчивое функционирование ЗОКИИ при проведении в отношении них компьютерных атак. Система безопасности включает в себя правовые, организационные, технические и иные меры и должна соответствовать требованиям, предъявляемым к:
   - силам обеспечения безопасности ЗОКИИ – создание структурного подразделения или назначение работников, ответственных за обеспечение безопасности ЗОКИИ, с соответствующими функциями и квалификацией;
   - программным и программно-аппаратным средствам – для обеспечения безопасности ЗОКИИ должны применяться средства защиты информации, сертифицированные на соответствие требованиям безопасности, или средства, прошедшие оценку соответствия; средства защиты информации должны быть обеспечены технической поддержкой;
   - организационно-распорядительным документам по безопасности ЗОКИИ;
   - функционированию системы безопасности в части организации работ по обеспечению безопасности ЗОКИИ – внедрение процессов планирования и реализации мероприятий по обеспечению безопасности ЗОКИИ, контроль состояния и совершенствование безопасности ЗОКИИ.

2. Выполнение требований по обеспечению безопасности ЗОКИИ. Для этого субъект должен:
   - определить требования к обеспечению безопасности ЗОКИИ в соответствии с его категорией значимости;
   - разработать и внедрить организационные и технические меры по обеспечению безопасности ЗОКИИ;
   - обеспечить безопасность ЗОКИИ в ходе его эксплуатации, а также при выводе из эксплуатации.

   Субъект КИИ может реализовывать меры по обеспечению безопасности самостоятельно либо с привлечением сторонних организаций, имеющих соответствующие лицензии.

K2 кибер безопасность

AM ANTI-MALWARE

ГосСОПКА: что это и для чего необходима

Все субъекты КИИ, независимо от наличия значимых объектов КИИ, должны осуществлять взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА). ГосСОПКА представляет собой единый территориально распределенный комплекс, включающий силы и средства для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Основной организационно-технической составляющей ГосСОПКА являются центры обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее – центры), организованные по ведомственному и территориальному принципам.

Структура ГосСОПКА:

- главный центр ГосСОПКА – национальный координационный центр по компьютерным инцидентам (НКЦКИ);
- ведомственные центры – создаются заинтересованными органами государственной власти;
- корпоративные центры – могут создаваться государственными корпорациями, операторами связи и другими организациями, осуществляющими лицензируемую деятельность в области защиты информации.

Цель взаимодействия субъекта КИИ с ГосСОПКА – обмен информацией о компьютерных инцидентах между субъектами КИИ, а также между уполномоченными органами иностранных государств и другими иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

В случае возникновения компьютерного инцидента на объекте КИИ субъект направляет в ГосСОПКА следующую информацию:

- дата, время, место нахождения или географическое местоположение объекта КИИ, на котором произошел компьютерный инцидент;
- наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой;
- связь с другими компьютерными инцидентами (при наличии);
- технические параметры компьютерного инцидента;
- последствия компьютерного инцидента[6].

Информация может быть передана с использованием технической инфраструктуры НКЦКИ либо посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте http://cert.gov.ru.

Срок передачи информации об инцидентах, связанных с функционированием ЗОКИИ, не позднее 3 часов с момента обнаружения, для иных объектов КИИ – не позднее 24 часов. После проведения мероприятий по реагированию на инциденты и ликвидации последствий компьютерных атак в отношении ЗОКИИ субъект информирует НКЦКИ о результатах проделанной работы в срок не позднее 48 часов после завершения таких мероприятий[7].

Кроме того, субъект КИИ, владеющий ЗОКИИ, в срок не позднее 90 календарных дней со дня включения данного объекта в реестр значимых объектов должен разработать план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также не реже одного раза в год проводить тренировки по отработке мероприятий плана.

При наличии потребности субъект КИИ может создать собственный центр ГосСОПКА. Для создания такого центра необходимо установить средства ГосСОПКА: средства обнаружения, предупреждения, ликвидации последствий компьютерных атак; средства поиска признаков компьютерных атак в сетях электросвязи, используемых для взаимодействия объектов КИИ, средства обмена информацией и криптографические средства защиты информации, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

Технические, программные и программно-аппаратными средства должны соответствовать требованиям, предъявляемым к средствам ГосСОПКА[8], а также должны соблюдаться порядок, технические условия установки и эксплуатации таких средств[9].

Если создание собственного центра ГосСОПКА не входит в планы субъекта, для осуществления мероприятий по обнаружению, предупреждению, ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты могут привлекаться сторонние организации, являющиеся аккредитованными центрами ГосСОПКА[10].

Дополнительные меры по обеспечению безопасности

В соответствии с Указом Президента № 250[11] с 1 января 2025 года субъектам КИИ запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними. Кроме того, с 1 января 2025 года субъектам КИИ, подпадающим под действие 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц»[12], запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах КИИ[13].

Также на основании Указа Президента № 250 ФСБ России определила порядок мониторинга защищенности информационных ресурсов, принадлежащих субъектам КИИ либо используемых ими. Мониторинг осуществляется Центром защиты информации и специальной связи ФСБ России и территориальными органами безопасности в отношении ИР, непосредственно подключенных к сети Интернет и (или) сопряженных с нею с использованием технологии трансляции сетевых адресов. Для проведения мониторинга субъекты КИИ должны направить до 1 сентября 2023 года на адрес электронной почты monitoring@fsb.ru сведения о доменных именах и внешних сетевых адресах ИР. В течение 7 рабочих дней необходимо уведомлять об их изменении, а также о приобретении (начале использования) доменных имен и внешних сетевых адресов новых ИР[14].

Контроль

Контроль за реализацией требований обеспечения безопасности объектов КИИ осуществляет ФСТЭК России путем проведения плановых и внеплановых проверок.

Плановые проверки проводятся каждые три года с момента внесения сведений об объекте КИИ в реестр значимых объектов КИИ.

Основанием для осуществления внеплановой проверки является:

- истечение срока выполнения субъектом КИИ выданного ФСТЭК России предписания об устранении выявленного нарушения требований по обеспечению безопасности ЗОКИИ;
- возникновение компьютерного инцидента на ЗОКИИ, повлекшего негативные последствия;
- приказ (распоряжение) руководителя ФСТЭК России, изданный в соответствии с поручением Президента РФ или Правительства РФ либо на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

Ответственность

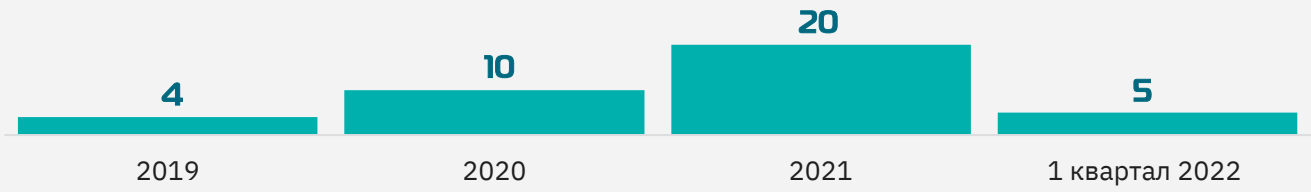
За нарушение требований законодательства в сфере обеспечения безопасности КИИ предусмотрены следующие виды ответственности:

1. Уголовная ответственность с наказанием в виде лишения свободы на срок вплоть до 10 лет за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ или ИС/ИТС/АСУ, относящихся к КИИ, либо правил доступа к указанной информации и объектам КИИ[15];

2. Административная ответственность:

Нарушение	**Размер штрафа для должностных лиц**	**Размер штрафа для юридических лиц**
Непредоставление/нарушение сроков предоставления во ФСТЭК сведений о результатах категорирования	10 - 50 тыс. руб.	50 - 100 тыс. руб.
	Повторное правонарушение – 50 - 100 тыс. руб.	Повторное правонарушение – 100 - 200 тыс. руб.
Непредоставление/нарушение порядка или сроков предоставления в ГосСОПКА информации, установленной законодательством	10 - 50 тыс. руб.	100 - 500 тыс. руб.
Нарушение требований к созданию систем безопасности ЗОКИИ и обеспечению их функционирования либо требований по обеспечению безопасности ЗОКИИ	10 - 50 тыс. руб.	50 - 100 тыс. руб.
Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении ЗОКИИ	10 - 50 тыс. руб.	100 - 500 тыс. руб.
Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ, а также между субъектами КИИ, и уполномоченными органами иностранных государств и иными иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты	20 - 50 тыс. руб.	100 - 500 тыс. руб.

Статистика по судебным решениям с вынесенными по статье 274.1 УК РФ приговорами:



Выполнение требований 187-ФЗ – резюме

Кратко процесс выполнения требований законодательства в области обеспечения безопасности критической информационной инфраструктуры можно описать следующим образом:

1. Определить, является ли организация субъектом КИИ.
2. Составить перечень объектов КИИ и направить его во ФСТЭК России.
3. В течении одного года после утверждения перечня объектов КИИ провести их категорирование и направить сведения о результатах категорирования во ФСТЭК России.
4. При наличии значимых объектов КИИ создать систему безопасности таких объектов и выполнить требования по обеспечению их безопасности в соответствии с категорией значимости. По решению субъекта требования по обеспечению безопасности могут применяться и для объектов КИИ, не отнесенных к значимым объектам.
5. Все субъекты КИИ должны организовать взаимодействие с ГосСОПКА: своими силами или использовать ведомственный или корпоративный центр.

ФСТЭК России осуществляет плановые проверки выполнения требований законодательства каждые 3 года, а также внеплановые в случае выявления нарушения, возникновения компьютерного инцидента, а также по поручению Президента РФ, Правительства РФ или по требованию прокурора.

За нарушение требований законодательства в области обеспечения безопасности КИИ предусмотрена административная и уголовная ответственность.

Использованные источники приведены в Приложении.

Приложение

[1] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[2] Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

[3] Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

[4] Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

[5] Приказ ФСТЭК России от 25.12.2017 N 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

[6] Приказ ФСБ России от 24.07.2018 N 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

[7] Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»

[8] Приказ ФСБ России от 06.05.2019 N 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»

[9] Приказ ФСБ России от 19.06.2019 N 281 Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»

[10] Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

[11] Указ Президента РФ от 01.05.2022 NN№ 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

[12] Федеральный закон от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц»

[13] Указ Президента РФ от 30.03.2022 N 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»

[14] Приказ ФСБ России от 11.05.2023 N 213 «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими»

[15] «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ, Ст. 274.1

02

ОПРОС СУБЪЕКТОВ КИИ

Оперативная ситуация

Все ли приступили к реализации требований ФЗ-187

Спустя шесть лет после принятия закона подавляющее число компаний приступили к выполнению требований ФЗ, при этом каждая десятая компания только готовится к запуску работ.

Основные препятствия — сложность понимания ФЗ и внутренние трудности с выстраиванием организационных процессов. Представителям ИБ-подразделений зачастую сложно обосновать руководству необходимость работ, найти финансирование, трактовать требования закона и приказов, в отдельных случаях компаниям сложно определить, являются ли они субъектом КИИ.

Вы приступили к работам по реализации требований ФЗ-187?

Отдельную проблему составляет сложность обоснования работ перед ответственными за блок АСУ ТП. Их основная задача – обеспечить работоспособность систем АСУ ТП. Негативный опыт внедрения сторонних средств в работающую систему заставляет сопротивляться подобным проектам. Решением может быть использование СЗИ, сертифицированных на совместимость с АСУ ТП. Однако такие сертификаты подтверждают совместимость определенных версий СЗИ и версий АСУ ТП. И попытки внедрения других версий этих решений также могут вызвать противодействие специалистов АСУ ТП.

«Стремительное развитие продуктовых линеек российских производителей как решений АСУ ТП, так и других может приводить к проблемам их совместимости с продуктами по защите технологических сетей. С другой стороны, эта же стремительность может приводить к существенным сложностям с точки зрения устойчивости и защищенности таких систем. Поэтому один из возможных вариантов решения данной проблемы – это наличие постоянно действующих лабораторий тестирования, в которых будут проводиться не просто тесты на совместимость конкретных устройств, но и проверки работоспособности систем в целом», – комментирует Михаил Кадер, архитектор решений по информационной безопасности Positive Technologies.

На каком этапе реализации находятся проекты

Среди компаний, которые уже приступили к работам, только 7% полностью завершили проекты по созданию системы обеспечения информационной безопасности (СОИБ), удовлетворяющей требованиям 187-ФЗ. 14% находятся на завершающих этапах, 34% занимаются организационной работой и 35% только начинают или планируют начать эту деятельность.

Прогресс компаний по реализации требований ФЗ-187

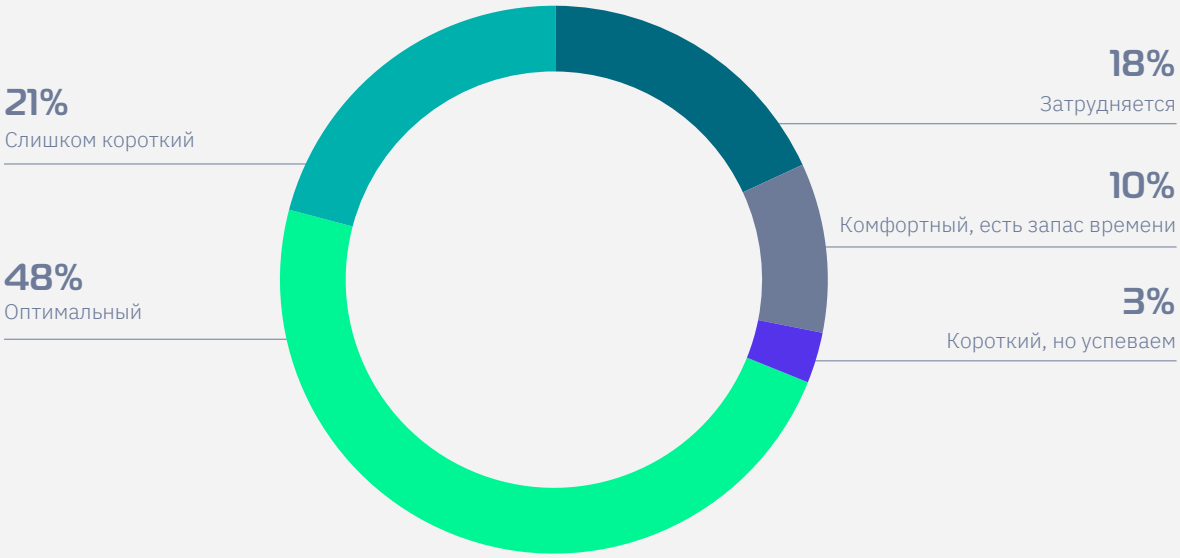
Успеют ли компании к указанному сроку

Больше половины опрошенных (58%) уверены в том, что срок, определенный в Указах №166 и №250, достаточен для того, чтобы реализовать все требования. При этом 21% компаний (каждая пятая) признаются, что не успеют реализовать проекты. Основным препятствием они называют сложности с заменой иностранных решений на отечественные, связанные как с высокой стоимостью, так и с нехваткой оборудования.

«Не редки ситуации, когда заказчиков не удовлетворяет функциональность отечественных решений. Однако многие вендоры готовы адаптировать свои решения под запросы крупных российских компаний. Более того, они начинают строить дорожную карту развития своих продуктов исходя из первоочередных потребностей заказчиков», – комментирует Егор Куликов, руководитель направления безопасности КИИ и АСУТП, К2 Кибербезопасность.

«С учетом того, что ряд компаний, включая нас, изначально ориентировались на конкурентоспособность и на российском, и на мировом рынках, отдельных задач по специальной доработке продуктов под потребности отечественных компаний не стояло. Запросы российских клиентов учитываются сразу. А вот настройки этих продуктов и индивидуальные подходы по внедрению комплексных систем обеспечения кибербезопасности на их базе встречаются регулярно. Особенно стоит выделить проекты по построению результативной кибербезопасности, то есть обеспечению киберустойчивости ключевых функций и бизнес-процессов предприятий, министерств и ведомств», – отмечает Михаил Кадер, архитектор решений по информационной безопасности Positive Technologies.

Как вы оцениваете срок, определенный Указом №166?



Сложности при реализации проектов

Только 29% опрошенных заявляют, что еще не столкнулись с серьезными сложностями на различных этапах реализации проекта. Основной проблемой является подбор и закупка отечественного ПО и оборудования, в частности замена МСЭ и инфраструктурного оборудования – с ней сталкиваются 27% компаний. 5% испытывают сложности с выделением финансирования. Остальные проблемы связаны с недостатком понимания ФЗ (13%), организацией процессов (8%) – выделением ответственных лиц за реализацию проекта, построением внутренних процессов обследования инфраструктуры и категорирования, подготовки документов, и кадровым голодом (8%).
У 8% компаний вызывает сложности процесс аудита и категорирования, а именно определение объектов аудита и оценка их категории значимости.

Все это в совокупности указывает на потребность в услугах аудита, которые помогут справиться с возникающими сложностями.

«Мы часто сталкиваемся с запросами, когда заказчику необходимо привести свою систему в соответствие требованиям законодательства, но он не понимает, с чего начать и какую последовательность шагов затем предпринять, – комментирует Егор Куликов, руководитель направления безопасности КИИ и АСУТП, К2 Кибербезопасность. – В этой ситуации мы приходим на помощь и формируем для заказчика индивидуальную дорожную карту, которая может включать обследование и категорирование объектов КИИ, подготовку документов для ФСТЭК, проектирование и внедрение системы защиты. Реализовать эту дорожную карту самостоятельно или отдать все или часть работ на аутсорсинг – решает заказчик».

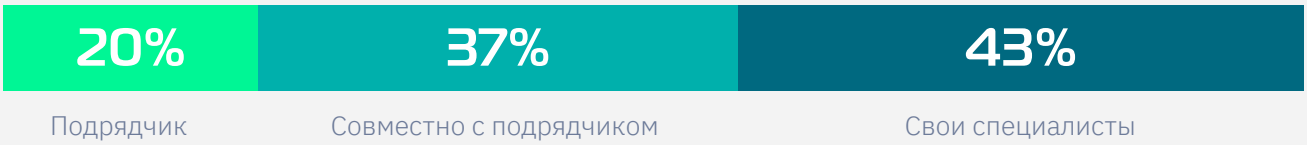
Трудности реализации проектов

Востребованность услуг сторонних организаций при реализации проектов

Чаще всего компании самостоятельно занимаются обследованием инфраструктуры и категорированием объектов КИИ (43%). Это связано с тем, что при категорировании подрядчику необходимо передать не только информацию об объектах АСУ ТП, но и такие чувствительные данные, как экономические показатели, данные о критичных процессах и др., которыми далеко не все компании готовы делиться.

Однако многие компании частично разделяют ответственность с подрядчиком (37%), и только 20% полностью передали свои задачи по категорированию объектов и подготовке документации на аутсорсинг.

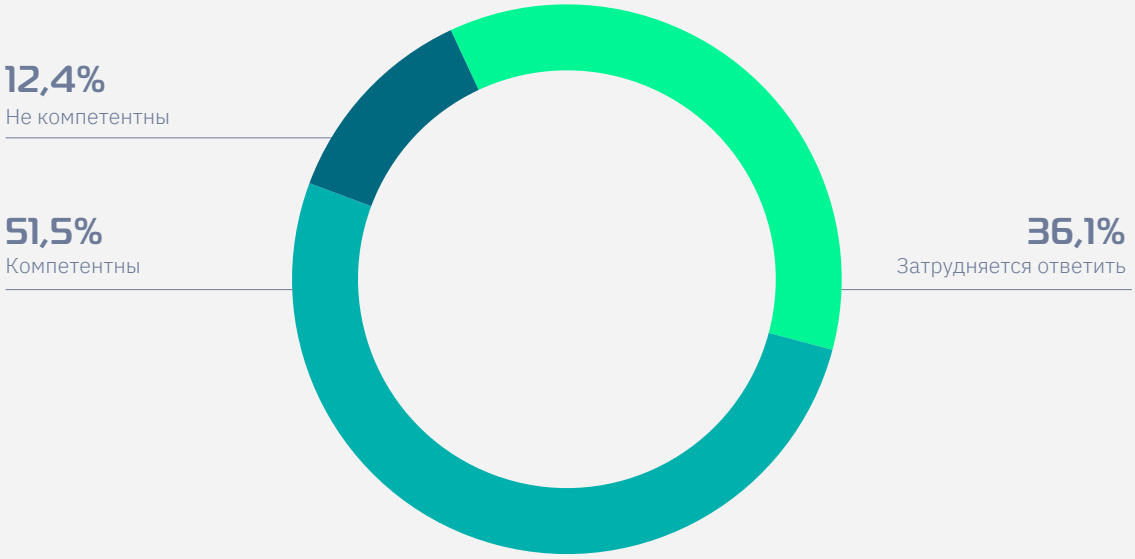
Кто проводит обследование и категорирование объектов в вашей компании?



Недоверие к аутсорсингу связано со слабой уверенностью в компетентности компаний, предоставляющих услуги обследования инфраструктуры и категорирования объектов — только половина опрошенных (51,5%) отметили высокий уровень доверия подрядчикам, 12,4% указали на то, что совсем не доверяют компаниям-аутсорсерам и предпочтут делать все самостоятельно.

Такие результаты связаны в первую очередь с тем, что сторонним специалистам часто не хватает отраслевой компетенции и понимания специфики инфраструктуры заказчиков. Также упоминаются спорные моменты в присвоении значимости объекта — подрядчик может злоупотреблять оценкой для того чтобы завысить стоимость организации СОИБ.

Как вы оцениваете компетенции компаний, оказывающих услуги по обследованию и категорированию?



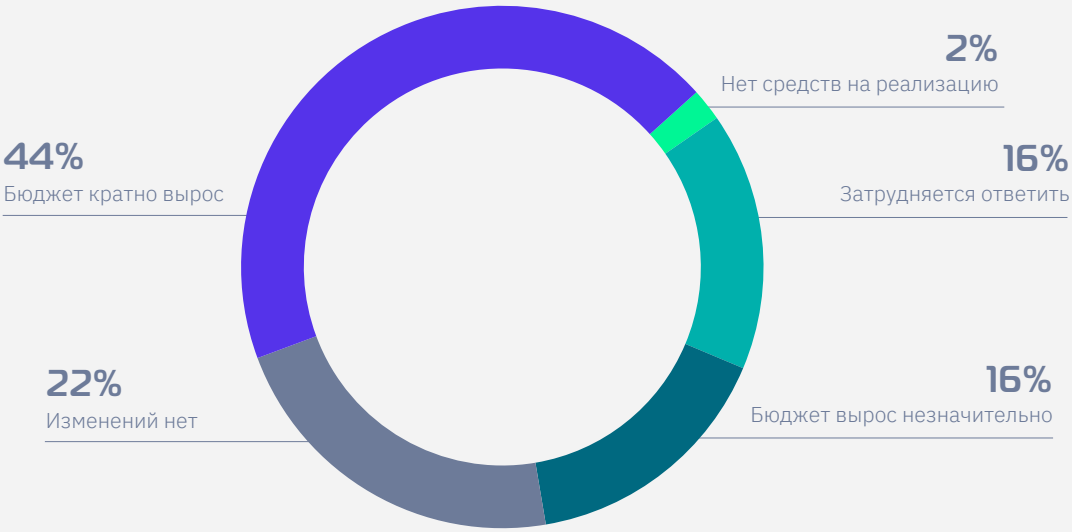
K2 кибер безопасность

ANTI-MALWARE

Расходы на реализацию проектов

Закон и сжатые сроки его обязательного исполнения вынудили компании увеличивать расходы на безопасность. Только 22% компаний остаются в рамках бюджетов за счет того, что заблаговременно подошли к их планированию, в то время как 2% компаний указали на то, что у них в принципе не хватает средств на реализацию.

Как требования ФЗ-187 повлияли на бюджет ИБ?



В большинстве случаев респонденты давали общую оценку увеличения затрат, не называя их реальных объемов. 14% компаний были вынуждены поднять бюджеты в 10 раз.

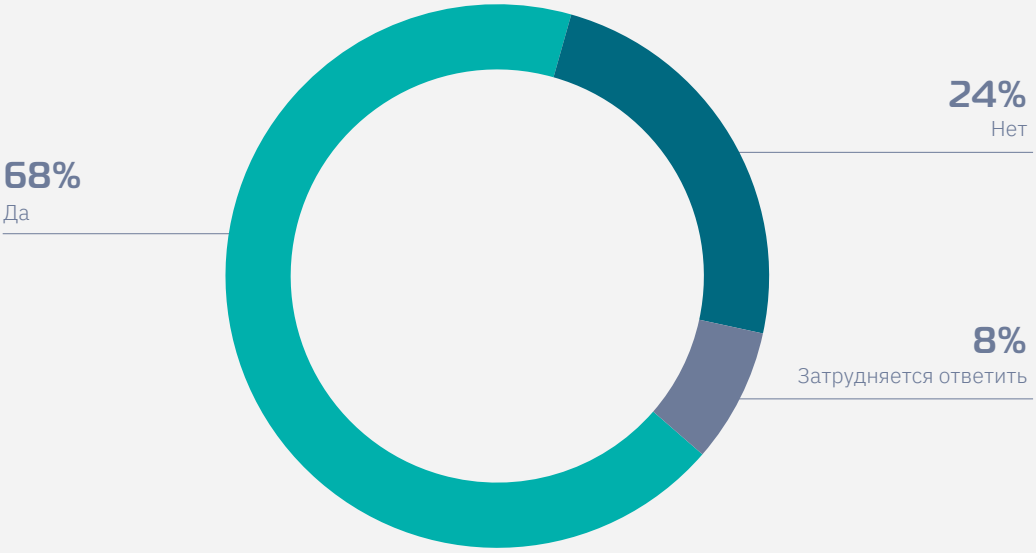
Увеличение бюджета связано с рядом причин. Так, недостаточно глубокий аудит приводит к тому, что объем работ оказывается недооценен. Объем работ может увеличиваться в силу технических особенностей инфраструктуры, когда невозможно разделить системы с разной категорией значимости. Кроме того, в некоторых компаниях в начале проекта нет полного понимания требований законодательства, что в дальнейшем приводит к росту числа необходимых СЗИ.

Чаще всего указывалась стоимость проекта в размере нескольких десятков миллионов рублей. Крупный бизнес гораздо точнее оценивает свои расходы. Большинство респондентов из небольших предприятий (с выручкой до 10 млрд руб. в год) не смогли дать оценку своих затрат.

Планы по закупкам

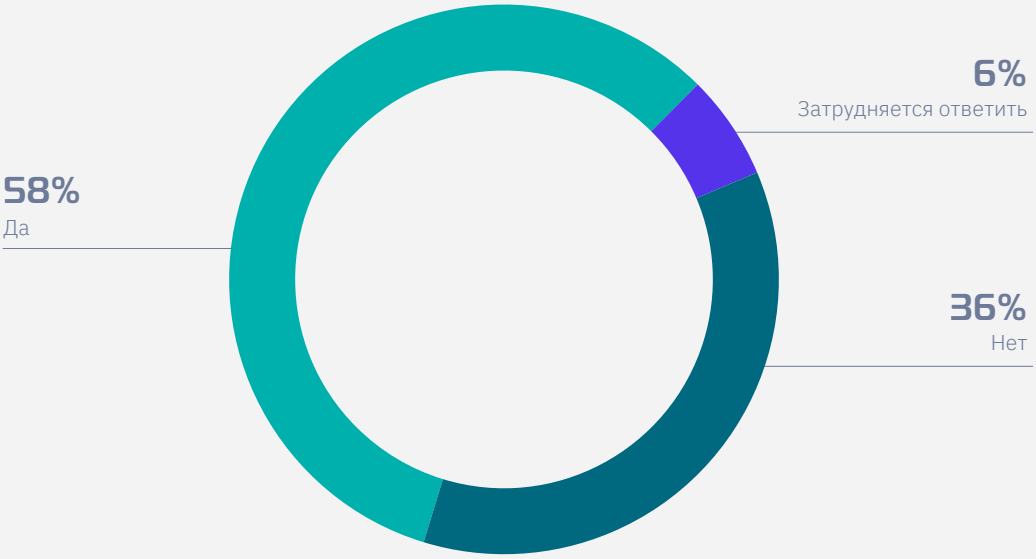
Значительное число компаний еще не знают, какие решения им понадобятся для реализации требований ФЗ — с планами не определились 24% респондентов. Четкое представление о предстоящих закупках имеют 68% опрошенных.

Понимает ли ваша компания, какие решения необходимы для реализации требований ФЗ?



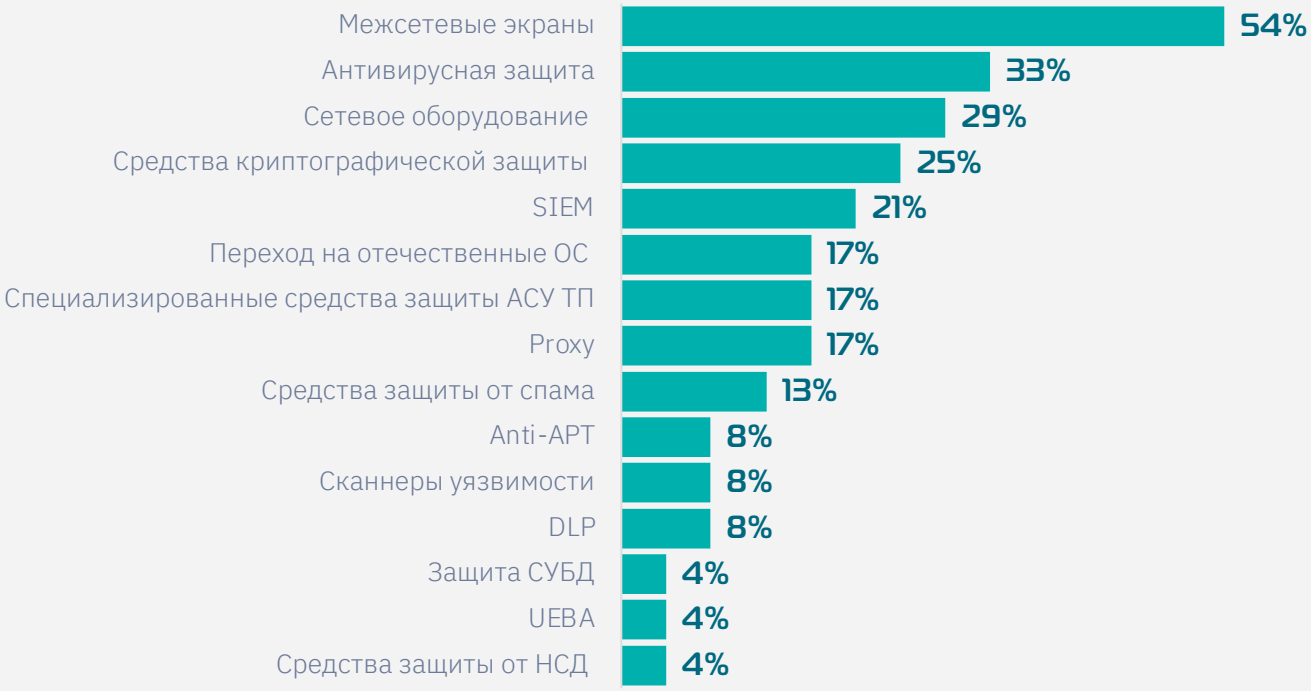
При этом 58% компаний уверены, что на рынке представлены все необходимые продукты для реализации проектов.

Как вы считаете, все ли необходимые продукты представлены на рынке?



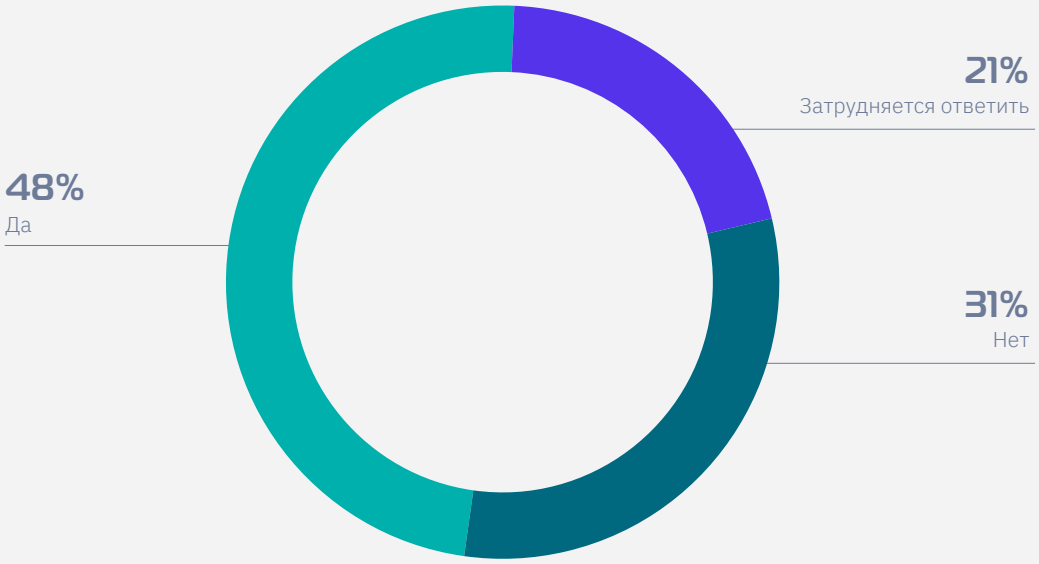
Всего выделено 8 классов решений, которые респонденты рассматривают для приобретения или уже тестируют. Наиболее востребованные классы – МСЭ, сетевое оборудование (базовое инфраструктурное) и SIEM.

Востребованные решения



При этом только 48% опрошенных уверены в том, что отечественные решения способны справиться с предъявляемыми требованиями, а 31% опрошенных категорически не удовлетворены тем, что предлагает рынок.

Способны ли отечественные решения справиться с предъявляемыми требованиями?



K2 кибер безопасность

AM ANTI-MALWARE

Мы дополнительно спросили у респондентов, недовольных отечественными решениями, что именно их не устраивает в продуктах. Основной проблемой является бедная функциональность по сравнению с импортными продуктами – этим не удовлетворены 27% опрошенных.

23% респондентов указали на то, что функциональность в принципе не соответствует заявленной производителем, в чем они убедились в результате тестирования.

20% уверены, что на рынке просто нет замены иностранным решениям.

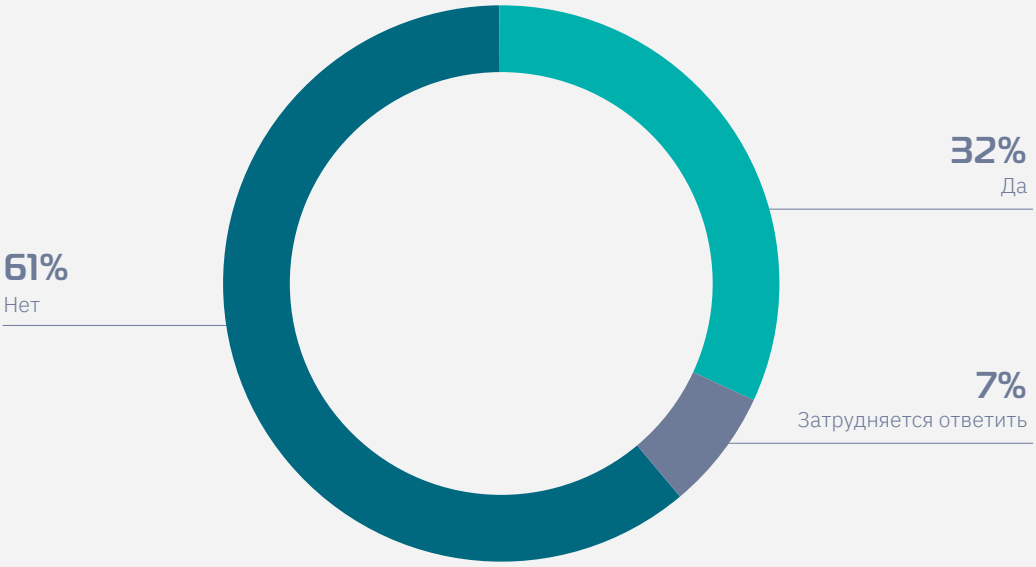
Надо отметить, что рынок отечественных ИБ-решений активно развивается последние годы. Вендоры работают над тем, чтобы обогащать возможности своих продуктов в ответ на потребности заказчиков, повышать уровень их зрелости.

Чтобы дать более полное представление о ситуации на рынке, мы опросили вендоров решений по защите КИИ. Результаты опроса представлены в Главе 3.

Опыт и оценка рисков безопасности

32% опрошенных субъектов КИИ сталкивались с инцидентами безопасности разной степени серьезности.

Сталкивались ли субъекты КИИ с инцидентами ИБ?



При этом минимум 35% инцидентов влекут за собой ущерб, который можно оценить в финансовых потерях.

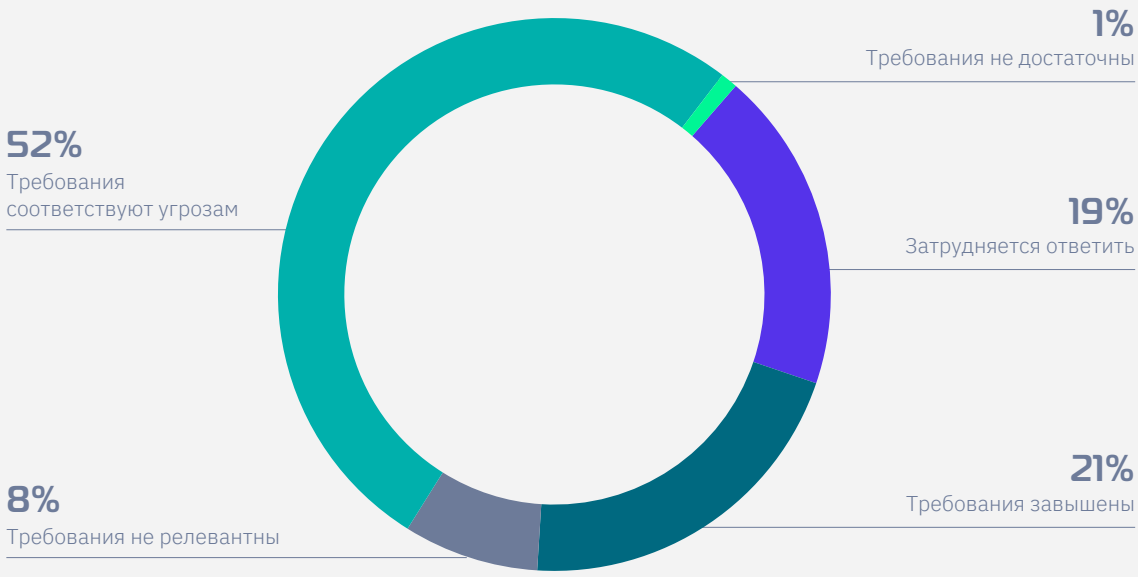
Простои — наиболее частое последствие инцидентов, причиной которых называют в основном DDoS-атаки и взломы сайтов. Кроме этого, приводятся следующие негативные последствия:

- Репутационный ущерб
- Потеря данных без восстановления
- Прямой финансовый ущерб

Отношение к требованиям ФЗ и его оценка

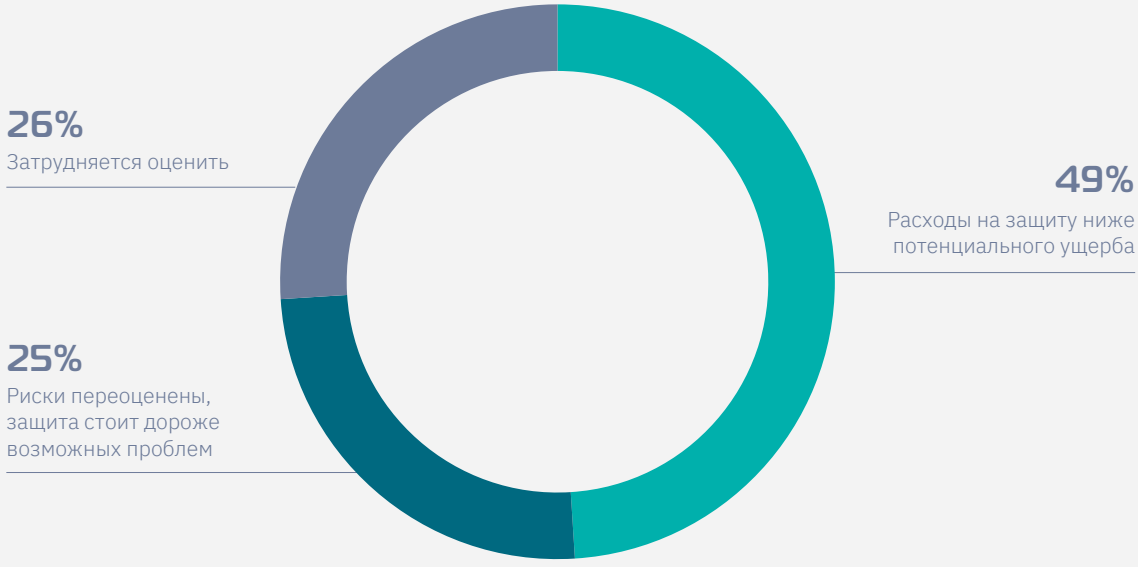
Мы попросили респондентов дать оценку требованиям ФЗ-187. Только половина опрошенных (52%) считают, что требования соответствуют реальным угрозам. 21% указали на то, что требования завышены и справедливы только для небольшого количества компаний. 8% считают, что ФЗ носит излишне бюрократический характер и что работа по нему больше направлена на «бумажную» безопасность, чем на отработку реальных угроз.

Как вы оцениваете справедливость требований, заложенных в нормативной документации по КИИ



Доля тех, кто согласен с обоснованностью расходов, чуть ниже. 49% респондентов считают, что потенциальные последствия инцидентов могут обойтись дороже, чем расходы на защиту.

Как вы оцениваете соответствие расходов на безопасность потенциальным рискам?



K2 кибер безопасность

AM ANTI-MALWARE

03

ЗАЩИТА КИИ КАК РЫНОК

Для достижения поставленных государством целей необходимо тесное сотрудничество регуляторов, бизнеса и поставщиков продуктов и решений. Учитывая рост числа компаний, который подпадают под действие ФЗ-187, и разнообразие потребностей, субъектов КИИ можно рассматривать как отдельный рынок. Для более полного представления об этом рынке мы решили опросить не только потребителей, но и игроков — компании, которые разрабатывают ИБ-решения, оказывают услуги по обследованию и категорированию объектов КИИ и реализации проектов создания СОИБ.

В исследовании приняли участие

АЙТИБАСТИОН · ASP · ГАРДА ТЕХНОЛОГИИ · КОД безопасности · kaspersky · positive technologies · R-Vision · Security Vision · UserGate · INFOWATCH

Продукты

Учитывая сложность проектов и требования по импортозамещению, компании вынуждены закупать дополнительные решения и заменять существующие. Уже сейчас виден большой спрос на основные классы продуктов:

- Антивирусы
- МСЭ
- Системы анализа защищенности
- Создание защищенных каналов связи
- IDS/IPS
- SIEM

Одновременно растет интерес к решениям, которые пока не получили широкого распространения в промышленности: PAM, SOAR, XDR, организация удаленного доступа к объектам КИИ.

Вступление ФЗ-187 в действие в 2018 году и последующие указы в 2022 году не были неожиданностью для вендоров благодаря выпущенному в 2014 году приказу ФСТЭК №31. Уже тогда стало ясно, что защита критической информационной инфраструктуры имеет важное значение для государства, и вендоры адаптировали стратегию разработки своих продуктов с учетом этого видения. Для вендоров ФЗ-187 оказался драйвером роста, так как дополнительно простимулировал спрос на их решения.

Часть вендоров начала разработку дополнительных продуктов, задачей которых является не работа непосредственно с рисками ИБ, а организационные задачи — автоматизация процессов ИБ, взаимодействие с ГосСОПКА, управление средствами ИБ и адаптация привычных корпоративных инструментов безопасности под специфику промышленных систем. Кроме этого, активно внедряются технологии машинного обучения, которые используются в системах мониторинга для выявления различных аномалий, уязвимостей в исходном коде и т.д.

Несмотря на неизбежно изоляционистский характер безопасности КИИ отечественные вендоры опираются на международную практику. У каждой страны есть свои особенности как в ИТ, так и в ландшафте угроз, их изучение позволяет обогащать свои решения и адаптировать иностранные практики к своим продуктам, что со временем позволит вывести их на международный уровень.

Информационная безопасность наиболее эффективна, когда доступен максимум информации, на которой можно построить матрицу пересечений и выявить лучшие практики. В этом плане можно отметить, что российский подход к организации процессов безопасности находится на международном уровне, в своих продуктах мы опираемся на практики безопасной разработки и, конечно, для наиболее эффективной работы нужно знать, что происходит в мире, и адаптировать знания под наши реалии. Как пример можно привести требования по гео-IP, которые у нас регламентированы и обязательны в новых требованиях ФСТЭК, но мало где применяются в мире.

Алексей Петухов
руководитель отдела развития
InfoWatch ARMA

Нейросети, ML, экспертные системы и другие технологии, которые обычно ассоциируют с искусственным интеллектом, давно используются практически во всех наших решениях, там, где они повышают эффективность продукта. Там, где нужно в большом потоке данных выделить аномалии и классифицировать их даже при отсутствии точных критериев классификации, а такие задачи решаются в наших FW, WAF, DBF, NTA, antiDDoS, DLP, DCAP и других системах, нейросети уже являются неотъемлемой частью архитектуры ядра продукта.

Рустэм Хайретдинов
заместитель генерального директора
группы компаний «Гарда»

Так как большая доля объектов КИИ являются промышленными объектами с набором специальных протоколов, которые не имеют широкого применения, то это заставляет производителей СЗИ разрабатывать и выпускать продукты, ранее не представленные на рынке. Тем не менее, пока на какую-то определенную роль не будет выпущен необходимый продукт, для реализации требуемых функций будут применять одно или несколько имеющихся на рынке решений. Например, пока продукты класса SOAR не были широко распространены, для решения соответствующих задач применялись другие продукты, не предназначенные напрямую для этого.

Алексей Дашков
директор Центра продуктового менеджмента
R-Vision

Тренды, барьеры развития рынка и их преодоление

Сертификация продуктов

Указ президента №250 вызвал всплеск активности производителей ПО и оборудования в части их сертификации

> Несмотря на некоторые послабления, предоставленные ФСТЭК, ускорения процесса сертификации не произошло — испытательные лаборатории не справляются с числом желающих пройти сертификацию. Процесс проверки соответствия продуктов требованиям по-прежнему занимает больше времени чем хотелось бы.
>
> **Константин Родин**
> руководитель направления
> по развитию продуктов
> АйТи Бастион

Тренды, барьеры развития рынка и их преодоление

Сложность трактовки ФЗ и нормативной документации

Многие клиенты испытывают трудности с интерпретацией закона. Сам ФЗ-187, правда, может звучать размыто, так как требования в нем описаны достаточно гибко, для того чтобы снизить риски монополизации, и можно сохранить гибкий подход при реализации проектов создания СОИБ. Поэтому аудитор, в портфеле которого уже есть проекты по защите КИИ, не испытывает сложностей с проецированием требований на инфраструктуру заказчика. При адекватном толковании требований можно эффективно снизить количество средств защиты, вопрос лишь в удобстве эксплуатации

Константин Родин
руководитель направления по развитию продуктов
АйТи Бастион

Те, кому приходится погружаться в документы регуляторов впервые, действительно испытывают очень большие сложности. Область ИБ на сегодняшний день имеет, в принципе, большое количество документов и связей между ними — тем более нужно понимать, как их трактовать и применять относительно специфики своего бизнеса. Очевидно, что со стороны регуляторов ведется очень хорошая работа – становится видно больше деталей и примеров, развиваются отдельные области, например по категорированию объектов, которое раньше вызывало много сложностей. Объем документации — основное препятствие для тех, кто не часто сталкивался с подобными задачами.

Алексей Петухов
руководитель отдела развития
InfoWatch ARMA

Тот корпус документов, который описывает системы защиты, достаточно неплох. Если мы говорим про процесс категорирования, то в нем есть множество нюансов, и заказчики могут испытывать трудности — в этой части мы ожидаем дополнений от отраслевых регуляторов, которые значительно облегчат задачи категорирования. Документация требует высокой квалификации, которая редко есть на местах, потому что просто не требуется, в связи с тем, что требования описаны гибко, и их может быть сложно проецировать при узкой специализации сотрудников.

Павел Коростелев
руководитель отдела продвижения продуктов
Код Безопасности

Мы видим существенное изменение подходов регуляторов в направлении практической, результативной кибербезопасности, в том числе и с точки зрения реализации конкретных подходов на предприятиях: начиная от ответственности руководства и заканчивая процессами оценки и подтверждения уровня защищенности.

Михаил Кадер
архитектор решений по информационной безопасности
Positive Technologies

Тренды, барьеры развития рынка и их преодоление

Короткие сроки

Срок 2025 год для решений СОИБ вполне реалистичен, большинство вендоров перешли на отечественные ОС, основная проблема состоит в аппаратных платформах. Полностью отказаться от импортной аппаратной части будет крайне сложно, и скорее всего ситуация вряд ли сильно изменится к 2025 году. Вероятно, можно ожидать дополнительных действий от регуляторов в этом вопросе.

Коммуникации между заказчиком и исполнителем

Заказчики и поставщики решений и услуг действительно имеют сложности в коммуникациях, особенно это касается проектов, в которых ведется работа с промышленными сетями и решениями — часто ответственной за реализацию проекта по защите назначается ИТ-служба, у которой низкая осведомленность в промышленной части инфраструктуры, поэтому необходимо привлекать специалистов АСУ ТП для более эффективного аудита и проектирования. Аудит также осложняется тем, что фактическая реализация инфраструктуры отличается от документированной, но это не является чем-то новым для крупных интеграционных проектов.

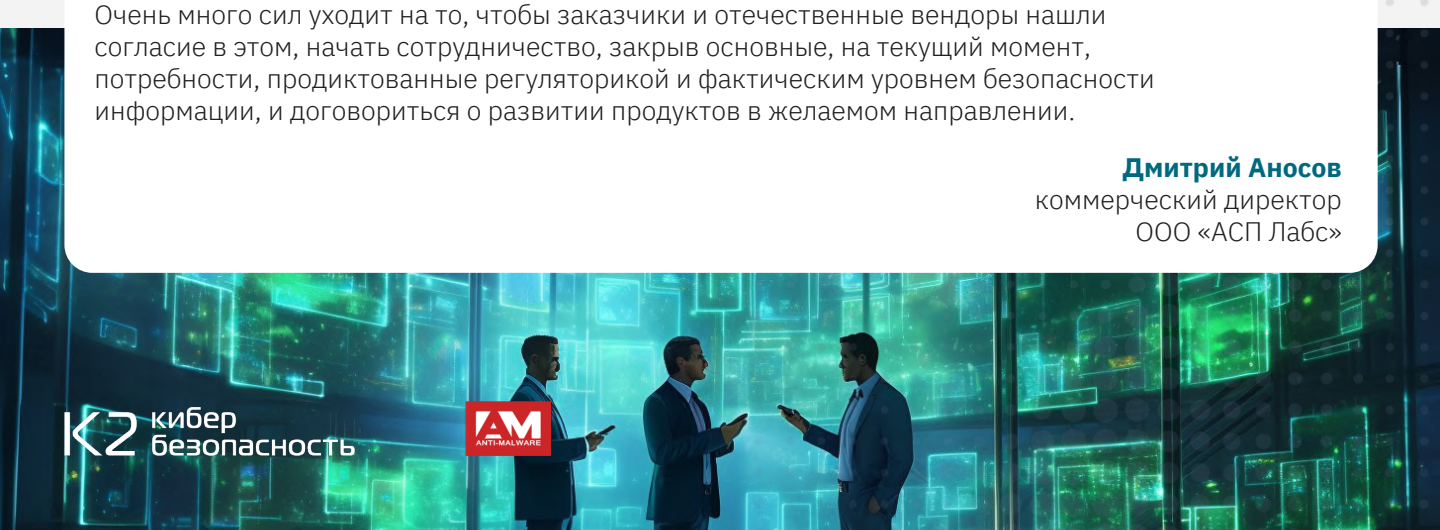
Мы занимаемся разработкой и внедрением систем автоматизации процессов ИБ, и хотелось бы лишний раз упомянуть пословицу, что, автоматизируя хаос, мы получим лишь автоматизированный хаос. Иначе говоря, перед внедрением систем автоматизации ИБ требуется прежде всего упорядочить, формализовать и адаптировать внутренние процессы ИБ заказчика, которые будут работать в связке с внедряемыми технологиями.

Руслан Рахметов,
генеральный директор
Security Vision

Отечественные решения, те же МСЭ, сильно отстают от аналогичных решений зарубежных компаний, которые ушли с рынка, по целому ряду параметров. У заказчиков существуют ожидания от продуктов, сформированные зарубежными вендорами за много лет. Многие заказчики предъявляют требования исходя из опыта работы с зарубежными продуктами, но если сконцентрировать внимание на конкретных технических задачах и определить фактическую потребность, то ее можно закрыть тем, что уже представлено на рынке.

Очень много сил уходит на то, чтобы заказчики и отечественные вендоры нашли согласие в этом, начать сотрудничество, закрыв основные, на текущий момент, потребности, продиктованные регуляторикой и фактическим уровнем безопасности информации, и договориться о развитии продуктов в желаемом направлении.

Дмитрий Аносов
коммерческий директор
ООО «АСП Лабс»



С годами мы наблюдаем значительное повышение уровня зрелости наших промышленных заказчиков в области информационной безопасности. Те проблемы, с которыми мы сталкивались ранее, такие как отрицание необходимости защиты систем управления технологическим процессом (АСУ ТП) и критической информационной инфраструктуры (КИИ), отсутствие ответственных лиц за обеспечение информационной безопасности, использование корпоративных решений для защиты АСУ ТП, теперь уходят на второй план. Тем не менее, развитие рынка ИБ промышленных инфраструктур диктует необходимость перехода от защиты объектов КИИ, в первую очередь, систем промышленной автоматизации, с использованием пассивного мониторинга, к более плотной интеграции средств защиты в периметр таких систем и реализации активных действий по реагированию на возникающие инциденты и (или) их недопущению. Повышение готовности заказчиков к реализации такого подхода в промышленных сетях – это то, над чем еще предстоит работать.

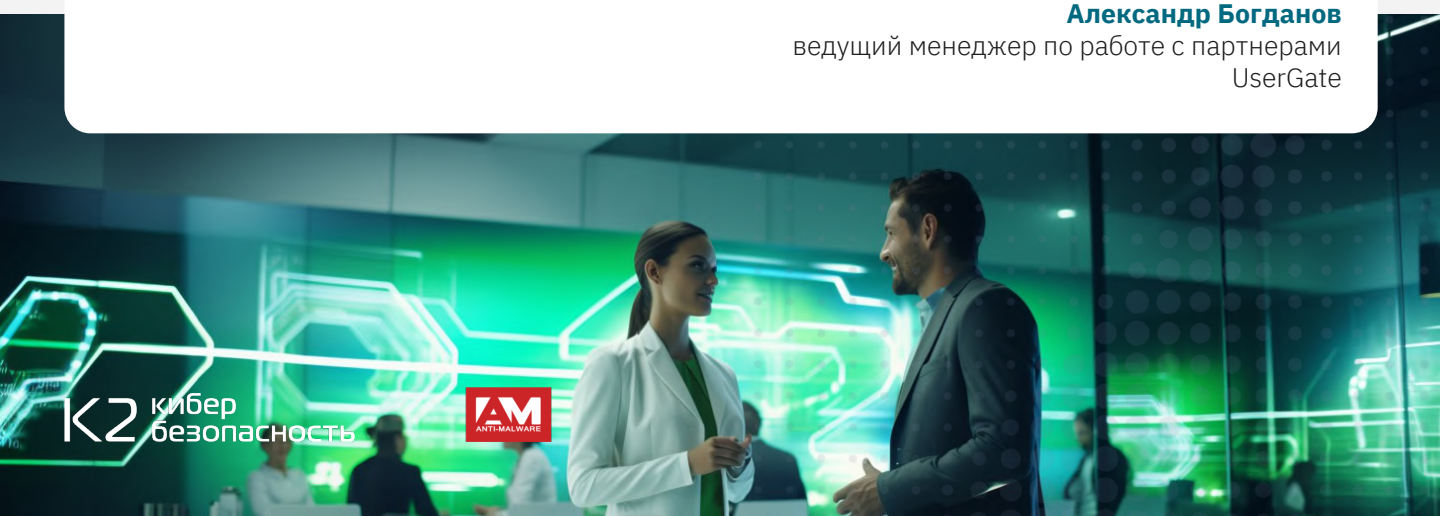
Андрей Бондюгин
руководитель группы по сопровождению
проектов защиты промышленных инфраструктур
«Лаборатория Касперского»

Заказчики испытывают опасения относительно отказоустойчивости и надежности решений — эти вопросы прорабатываются в каждом проекте отдельно, чтобы учесть все требования и разработать наиболее эффективный сценарий реализации внедрения продуктов. Также высокое значение имеет перенос старых политик безопасности и конфигураций на новые инфраструктуры — тут мы движемся в сторону автоматизации этого процесса.

Павел Коростелев
руководитель отдела продвижения продуктов
Код Безопасности

Сложности на проектах субъектов КИИ — такие же, как и при работе с любым другим заказчиком, можно сказать, что у них нет специфических задач, и часто разница только в масштабах. Главный вопрос, который сейчас стоит перед заказчиками, — переход с импортных решений, и для многих этот переход вынужденно резкий. Сети десятилетия строились на оборудовании конкретных производителей, и их очень сложно поменять в моменте. Поэтому для многих компаний большой труд – перенос конфигураций, адаптация сети к текущим стандартам и задачам. По этой причине вендору очень важно иметь зрелого партнера с хорошей технической компетенцией, который сможет не только грамотно настроить решения, но и обеспечить адекватную степень модернизации инфраструктуры, которая неизбежна при таких комплексных проектах.

Александр Богданов
ведущий менеджер по работе с партнерами
UserGate



Тренды, барьеры развития рынка и их преодоление

Проблема компетенций и нехватки кадров

О недостатке компетенций говорят все участники рынка. Кроме того, на рынке наблюдается дефицит специалистов по аудиту. Качество сбора данных во время аудита зависит от полноты предоставленной информации, особенно о том, какие процессы и каким образом влияют на экономические показатели. Часто этой информации просто нет из-за отсутствия у заказчика погруженных в тему сотрудников или ей делятся неохотно, считая ее чувствительной. Завышенные ожидания от подрядчиков пересекаются с тем, что клиент не может предоставить нужную информацию, отсюда возникает неудовлетворенность услугами. Решить эту проблему может только большая открытость всех участников процесса и обмен опытом между исполнителями, фасилитировать который способны либо государство, либо учебные центры.

Дефицит оборудования, проблемы миграции и совместимости

Почти все вендоры сталкиваются с нехваткой оборудования для организации даже пилотных внедрений. Основными факторами здесь являются снижение объемов поставок в результате санкций и жесткое требование быстрого импортозамещения, к которому многие оказались не готовы. Замена оборудования оказывается мучительным процессом: клиент должен понять, где взять оборудование в нужном количестве и по оптимальной стоимости. Кроме этого, сам процесс миграции затруднен тем, что инфраструктуры долгие годы строились на импортных решениях, из-за чего возникают трудности с переносом конфигураций и совместимостью. Многие производители уже адаптировали свои решения к отечественным операционным системам РЕД ОС, Astra Linux, AlterOS, ОСнова и др.

> Разработка средств защиты информации в компании не связана жестко с какой-либо отдельной проприетарной операционной системой. Среды разработки под системы в том числе с открытым исходным кодом полностью решают наши задачи. При острой необходимости возможно также применение кросс-сборки.
>
> **Рустэм Хайретдинов**
> заместитель генерального директора
> группы компаний «Гарда»

При этом большинство производителей ИБ-решений отзываются позитивно об отечественных разработках в области аппаратных платформ и не видят проблем, которые они не могли бы оперативно решить.

> Переходить на новые решения всегда сложно — у специалистов сформированы определенные привычки к продуктам, которые часто использовались, и адаптация занимает какое-то время. Мы проделываем большую работу над тем, чтобы сделать пользовательские сценарии более привычными и понятными, особенно в части сбора событий, настроек и переноса политик.
>
> **Алексей Петухов**
> руководитель отдела развития
> InfoWatch ARMA

Тренды, барьеры развития рынка и их преодоление

Актуальные вызовы кибербезопасности

Проблема сопряжения между собой СЗИ разных вендоров никуда не уходит, а только увеличивается по прошествии времени и выхода на рынок новых средств защиты. Поэтому наиболее перспективной стратегией видится не производство точечных средств защиты, а развитие единого комплекса средств безопасности.

Алексей Дашков
директор Центра продуктового менеджмента
R-Vision

В последнее время возросло количество кибератак на цепочки поставок, в результате реализации которых на стороне взломанной ИТ-компании хакеры внедряют вредоносный код в ПО, который затем незаметно попадает в инфраструктуру заказчиков, например, вместе с очередным обновлением. По уровню потенциального негативного воздействия такая кибератака действительно может сравниться со взломом значимого объекта КИИ, особенно ввиду того, что внедренный в ПО вредоносный модуль может попасть в инфраструктуры сразу множества субъектов КИИ. Одним из вариантов решения задачи могла бы стать организация государственного сервиса по проверке безопасности ПО и СЗИ, например, с использованием «песочниц», методов композиционного анализа и средств статического, динамического, интерактивного анализа; после такой проверки отсутствия «закладок» в дистрибутиве или пакете обновления значение хэш-суммы инсталлятора можно помещать в публично доступный реестр надежного софта, с которым субъекты КИИ будут сверяться в обязательном порядке.

Руслан Рахметов
генеральный директор
Security Vision

Тренды, барьеры развития рынка и их преодоление

Ожидаемые изменения в законодательстве и регуляции

Как известно, государство работает над множеством законов, но индустрия ИБ особо трепетно и с беспокойством ожидает появления требований на СЗИ, которые до сих не стандартизированы. Многих разработчиков это приведет к необходимости изменять и спешно дорабатывать, а в каких-то случаях и перерабатывать свои продукты. Другими ожидаемыми нормативными актами является реализация желания каждой отрасли, указанной в законе о КИИ, построить свой собственный ведомственный центр защиты информации, что безусловно повлияет на каждый объект КИИ.

Также после многочисленных подтвержденных фактов утечки персональных данных мы ожидаем внесение изменений в законодательство указанной области, что повлияет на средства обеспечения защищенности систем, обрабатывающих персональные данные.

Алексей Дашков
директор Центра продуктового менеджмента
R-Vision

В ближайшее время можно ожидать окончательного формирования перечня типовых отраслевых объектов КИИ со стороны отраслевых комитетов и индустриальных центров компетенций и разработку проекта системы оценки технологической независимости объектов КИИ со стороны Минцифры, а далее для типовых объектов КИИ будут определены сроки замещения импортного ПО. Также ожидается существенное расширение перечня организаций, подпадающих под требования законодательства о безопасности КИИ.

В настоящий момент регуляторные полномочия несколько размыты между Минцифры, ФСТЭК России и ФСБ РФ, и это не считая отраслевых регуляторов, например, ЦБ РФ. Консолидация полномочий в едином ведомстве, вероятно, пошла бы на пользу с точки зрения формирования единообразного подхода к требованиям и выпускаемым НПА, но в текущий момент такая задача, вероятно, не является первоочередной ввиду множества других важнейших задач, критичных с точки зрения кибербезопасности на уровне всего государства.

Руслан Рахметов
генеральный директор
Security Vision

С целью повышения доверия к используемому программному обеспечению уже развивается и будет развиваться в дальнейшем нормативная и методическая база по разработке безопасного программного обеспечения и отдельных процессов в рамках его разработки: использование инструментов статического, динамического и композиционного анализа, проведение разных видов тестирования и др. Будет осуществляться постепенный переход к конструктивной информационной безопасности, то есть безопасности, реализуемой в том числе на уровне архитектуры, замысла в средствах защиты и других программно-аппаратных комплексах, называемых в «Лаборатории Касперского» кибериммунными решениями. В ближайшем будущем мы ожидаем усиление контрольных функций со стороны отраслевых регуляторов в области информационной безопасности.

Андрей Стрелков
руководитель направления развития продуктов для промышленной безопасности
«Лаборатория Касперского»

04

ЗАКЛЮЧЕНИЕ

Безопасность КИИ — масштабный вопрос государственного уровня, одновременно с этим обеспечение защиты субъекта КИИ — комплексный проект, включающий в себя обследование инфраструктуры, взаимодействие со ФСТЭК, разработку большого количества документации и организационных мер, закупку средств защиты и оборудования, их внедрение и создание системы обеспечения информационной безопасности (СОИБ). Во всех процессах задействовано большое количество сторон со своими разными, иногда противоречивыми, интересами, и главным решением на пути к желаемому уровню безопасности является достижение взаимопонимания всех этих сторон.

Как показывают результаты исследования, ситуация с обеспечением безопасности КИИ позитивная, несмотря на серьезные трудности, с которыми сталкивается бизнес. Сроки выполнения поставленных государством задач большинство опрошенных воспринимают как оптимальные и выполнимые, большинство также уже понимает, какие средства предстоит приобрести, и считают, что смогут это сделать.

Сложившаяся экономическая и политическая ситуация дала компаниям мощный импульс озаботиться своей безопасностью. Спрос на услуги аудита начал резко расти сразу после выхода Указа №250 — по нашим оценкам, рост спроса со стороны субъектов КИИ составил 70% по отношению к аналогичному периоду 2021-2022 годов. На текущий момент также наблюдается большой спрос на проектирование систем защиты, во многих случаях даже раньше окончания работ по определению категорий объектов КИИ. Компании торопятся успеть к сроку, примерно представляя, к какой категории будут отнесены объекты в их инфраструктурах.

Многие эксперты уверены, что спрос сохранится на том же уровне и после 2025 года, но на непродолжительный период, а затем будет поддерживаться потребностями в поддержке и развитии существующих проектов.

События начала прошлого года дали толчок к развитию не только на рынке ИБ. Так, например, программа импортозамещения, запрет использования зарубежных средств в составе критической информационной инфраструктуры подтолкнули к развитию также и рынок отечественных решений в области промышленной автоматизации. Естественно, в своем развитии вендоры систем промышленной автоматизации будут постепенно переходить на более новые, более современные технологии. В свою очередь, использование новых технологий потребует адаптации средств и технологий обеспечения безопасности информации. Уже сейчас видно, что крупнейшие отечественные вендоры решений в сфере ИБ АСУ ТП расширяют функциональность своих продуктов в сторону менеджмента ИБ. Если в корпоративных сетях уже идет процесс централизации и автоматизации управления ИБ , то в АСУ ТП это недалекое будущее. У промышленных компаний будет расти потребность выводить ИБ АСУ в единое поле безопасности, вместе с корпоративными сетями.

Соответственно, будет расти спрос на услуги аутсорсинга ИБ, услуги SOC. И, безусловно, тут выиграют те, кто первым сможет предложить комплекс услуг, максимально адаптированных под нужды производства.

Дмитрий Аносов
коммерческий директор
ООО «АСП Лабс»

Высокие затраты на исполнение требований закона не обязательно должны рассматриваться как откуп перед регуляторами. Текущая ситуация, в которой мы сейчас находимся, и бурное развитие информационной безопасности позволяет компаниям выйти на более осознанный уровень понимания ИБ и ее роли в бизнесе как инструмента увеличения прибыли. В какой-то момент отпадет необходимость в такой жесткой регуляции. Скорее всего это произойдет, когда компании начнут развивать свои бизнес-функции с учетом возможностей ИБ-решений, которые позволяют делать процессы более прозрачными и контролируемыми, оптимизируя операционные расходы, и строить свои ИБ-процессы даже лучше того, как это требуют регуляторы.

Важно увидеть, что текущая ситуация – это определенная точка роста. Отношение к информационной безопасности меняется, важно понять, что те системы и инфраструктуры, которые мы сейчас строим – с нами надолго, и безопасность здесь – это надежность.

Алексей Петухов
руководитель отдела развития
InfoWatch ARMA

Рынок защиты КИИ будет прогрессивно расти, так как уход большого количества иностранных компаний, в числе которых оказалось множество производителей средств защиты информации, а также рост числа атак заставил многие компании в срочном порядке повышать уровень зрелости своих систем и одновременно противостоять большому количеству угроз. И тут важно понимать, что это задача не ближайшего будущего, это уже наше настоящее. И так как рост рынка происходит очень активно, мы ожидаем повышения конкуренции и появления новых имен в индустрии. Как-никак, без конкуренции нет развития.

Алексей Дашков
директор Центра продуктового менеджмента
R-Vision

Есть мнение, что примерно 80% ИБ-рынка России официально «освободилась» от «сбежавших» иностранных вендоров, но реальность такова, что многие и многие отечественные пользователи (в том числе субъекты КИИ) несмотря ни на что продолжают сидеть на старых зарубежных железках с необновляемым софтом. Неизбежно со временем весь этот парк иностранных NGFW окончательно станет неработающим устаревшим хламом. При этом важно понимать, что из отпущенных 3-5 лет на такую миграцию по инерции уже один год прошел...

И вот насколько велика сила инерции тех, кто не хочет ничего менять, настолько же активными были за этот год российские ИБ-вендоры — думаю, их доля по отношению к иностранным компаниям с 20% выросла примерно до 40-50%. Произошло это, в том числе, из-за того, что все понимают — необходимость миграции на российские решения является объективной неизбежностью, которая наступит. Не сразу, постепенно... но неотвратимо — как в связи с уходом иностранных вендоров, так и с Указом Президента РФ (№ 250 от 01.05.2022) «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Александр Богданов
ведущий менеджер по работе с партнерами
UserGate

Несмотря на серьезные трудности, с которыми сталкивается бизнес, ситуация с обеспечением безопасности КИИ позитивная. Но не стоит забывать, что в контексте КИИ речь идет о сотнях тысяч организаций. По нашему опыту, большое количество предприятий все еще используют зарубежные решения в инфраструктуре значимых объектов защиты, в том числе средства защиты. При этом мы видим тренд, что российские вендоры сейчас получили большой драйвер роста в связи с освободившимися продуктовыми нишами, а также поддержку от государства. Компании развивают свои продукты, при этом используют передовые технологии, доступные на рынке.

Андрей Заикин
директор по развитию бизнеса
К2 Кибербезопасность

K2 кибер безопасность

ANTI-MALWARE

Список сокращений

АСУ ТП – автоматизированная система управления техническими процессами

ГосСОПКА – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак

ЕГРЮЛ – Единый государственный реестр юридических лиц

ЗОКИИ – значимый объект критической информационной инфраструктуры

ИБ – информационная безопасность

ИР – информационный ресурс

ИС – информационная система

ИТ – информационные технологии

ИТС – информационно-телекоммуникационная сеть

КИИ – критическая информационная инфраструктура

МСЭ – межсетевой экран

НКЦКИ – Национальный координационный центр по компьютерным инцидентам

НСД – несанкционированный доступ

ОКВЭД – Общероссийский классификатор видов экономической деятельности

ПО – программное обеспечение

СЗИ – средство защиты информации

СОИБ – система обеспечения информационной безопасности

ТЗ – техническое задание

ФЗ – федеральный закон

ФСТЭК – Федеральная служба по техническому и экспортному контролю

K2 кибер безопасность

ANTI-MALWARE

Контакты для связи

pr@k2.tech