РАЗДЕЛ III

УПРАВЛЕНИЕ КИБЕРРИСКАМИ И КИБЕРБЕЗОПАСНОСТЬЮ

Задачи управления киберрисками и кибербезопасностью критических инфраструктур национального масштаба

А. А. Кононов, А. В. Сичкарук, К. В. Черныш

В современном обществе практически все инфраструктуры обеспечивающие жизнедеятельность используют *информационные технологии* (*кибертехнологии*), которые в свою очередь играют критическую роль практически в любой инфраструктуре. Очевидно, что в этих условиях значение *безопасности кибертехнологий* (кибербезопасности) в критических инфраструктурах современного общества (инфраструктурах госуправления, финансовой, банковской, транспортной, энергетического, ресурсного, коммунального и продуктового обеспечения) возрастает чрезвычайно.

В настоящее время в стране существуют надежные и доказавшие свою эффективность системы аттестации, сертификации и лицензирования отдельных объектов и средств обеспечения информационной безопасности. Их важность и значение трудно переоценить, но в тоже время можно констатировать, что эти системы не дают возможности получать полную всеобъемлющую картину состояния информационной безопасности (кибербезопасности) *критических инфраструктур национального масштаба* (*КИНМ*) и *национальных критических инфраструктур* (*НКИ*), что имеет особое значение для тех лиц и органов, которые несут ответственность за безопасность такого рода инфраструктур и которые в результате

зачастую оказываются в положении, когда их ответственность во много раз превышает их возможности контроля состояния кибербезопасности КИНМ и НКИ.

Далее для краткости будет использоваться только термин «национальная критическая инфраструктура», хотя следует отметить, что понятие **критической инфраструктуры национального масштаба** шире понятия **национальной критической инфраструктуры** и включает в себя помимо НКИ критические инфраструктуры коммерческих организаций национального и транснационального масштаба, для которых, однако, задачи управления кибербезопасностью и киберрисками будут в значительной степени такими же, что и для НКИ.

В связи с наличием дисбаланса в ответственности и возможностях контроля и *управления кибербезопасностью* (*УКБ*) НКИ встает задача создания таких систем УКБ НКИ, которые позволили бы устранить этот дисбаланс. Эти системы должны обеспечивать максимально возможный уровень доказанного доверия к кибербезопасности НКИ. Ниже предлагается перечень задач, которые должны решаться с помощью такого рода систем, составленный с учетом того, что целевые и оценочные установки (целевые функции) в управлении кибербезопасностью задаются посредством постановки и решения задач управления *рисками нарушения кибербезопасности* (*киберрисками*) и минимизации киберрисков, и, в свою очередь, задачи минимизации киберрисков могут эффективно решаться, если при оценке рисков обеспечивается возможность отслеживания источников их формирования и, насколько это возможно, предоставляются механизмы воздействия на эти источники.

Предполагается, что для решения указанных задач будет использоваться трехуровневая структура управления обеспечением кибербезопасности НКИ, включающая: *центральный уровень обеспечения кибербезопасности национальной критической инфраструктуры* (*ЦУОКБ НКИ*), *региональный уровень обеспечения кибербезопасности регионального сегмента НКИ* (*РУОКБ РСНКИ*), объектовый уровень обеспечения кибербезопасности *объекта НКИ* (ОНКИ).

Задачи управления киберрисками, которые должны решаться для обеспечения управляемости кибербезопасностью НКИ:

1. Построение типовых структурных моделей и типизация объектов НКИ. Решается на уровне ЦУОКБ НКИ.
2. Категорирование ОНКИ по опасности на основе общности моделей угроз по типам объектов НКИ. Построение типовых моделей угроз.

Оценка типовых рисков нарушения кибербезопасности НКИ. Решается на уровне ЦУОКБ НКИ.

3. Построение базовых профилей защиты (в данном контексте в широком понимании «профиля защиты», как системы всех возможных требований по кибербезопасности, а не только существующих в рамках предусмотренных ГОСТ Р ИСО/МЭК 15408) по категориям объектов НКИ с учетом типовых моделей угроз и существующей нормативно-правовой базы. Решается на уровне ЦУОКБ НКИ при взаимодействии с РУОКБ РСНКИ.
4. Контроль качества систем требований:
   - на адекватность;
   - на полноту «закрытия» наиболее опасных уязвимостей, угроз и возможных событий киберрисков;
   - на непротиворечивость;
   - на отсутствие избыточности;
   - на отсутствие деструктивного эффекта в отношении базовой функциональности и конкурентоспособности объектов НКИ.

   Решается при взаимодействии ЦУОКБ НКИ и РУОКБ РСНКИ.
5. Групповая или пообъектная конкретизация профилей защиты. Решается при взаимодействии РУОКБ РСНКИ с ЦУОКБ НКИ.
6. Доведение актуальных профилей защиты до объектов с возможностью экстренного доведения новых требований по безопасности. (ЦУОКБ НКИ → РУОКБ РСНКИ → ОНКИ).
7. Регулярный, на периодической (например, ежеквартальной) основе, и экстренный (в возможном экстренном режиме отчетности, в том числе, по новым требованиям доведенным в экстренном порядке) сбор отчетности о выполнении требований профилей защиты. (ОНКИ → РУОКБ РСНКИ → ЦУОКБ НКИ).
8. Обработка в режиме реального времени отчетов о выполнении требований по безопасности. Решается на уровне ЦУОКБ НКИ.
9. Оценка рисков доверия [5] к кибербезопасности НКИ. Идентификация уязвимостей, «узких мест», опасных сочетаний невыполняемых требований, формирование и обоснование комплексных национальных и региональных программ, мер и мероприятий по повышению кибербезопасности НКИ. Решается на уровнях ЦУОКБ НКИ и РУОКБ РСНКИ.

10. Инспекционный контроль достоверности предоставляемой отчетности о выполнении требований кибербезопасности. Проводится ЦУОБ НКИ и РУОБ РСНКИ на ОНКИ.

Основные преимущества предлагаемого подхода — обеспечение на уровне ЦУОБ НКИ полной и всеобъемлющей картины состояния кибербезопасности НКИ и обеспечение контроля и управляемости кибербезопасности НКИ.

Методология и средства автоматизации решения перечисленных задач разработаны в Институте системного анализа Российской академии наук и опробованы при решении задач обеспечения кибербезопасности реальных НКИ (банковской и транспортной) [1–4].

Литература

1. *Кононов А. А., Стрельцов А. А., Черешкин Д. С.* Защита критических секторов региональной информационной инфраструктуры // II Межрегиональная конференция «Информационная безопасность регионов России ИБРР-2001», Санкт-Петербург, 26–29 ноября 2001 г.: Материалы конференции. Т. 2. СПб., 2001. С. 18–25.
2. *Черешкин Д. С., Кононов А. А., Бурдин О. А.* Автоматизированная система мониторинга выполнения требований информационной безопасности // VIII Санкт-Петербургская Международная Конференция «Региональная информатика-2002», Санкт-Петербург, 26–28 ноября 2002 г.: Материалы конференции. Часть I СПб., 2002. С. 137.
3. *Кононов А. А.* Информационное общество: общество тотального риска или общество управляемой безопасности? // Проблемы управления информационной безопасностью: Сб. трудов. М.: УРСС, 2002. С. 6–20.
4. *Кононов А. А.* Управление безопасностью региональной информационной инфраструктуры // Проблемы управления информационной безопасностью: Сб. трудов. М.: УРСС, 2002. С. 36–53.
5. *Кононов А. А.* Оценка рисков доверия к кибербезопасности компьютеризированных систем // Проблемы кибербезопасности информационного общества: Труды Института системного анализа Российской академии наук: Т. 27. М.: КомКнига/URSS, 2006. С. 35–42.