МЕТОДИКА ОЦЕНКИ ПОЛИТИЧЕСКОЙ ЗНАЧИМОСТИ УГРОЗ ОБЪЕКТУ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ПРИМЕРЕ ОБЪЕКТА ИНФОКОММУНИКАЦИЙ

Е.В. Смирнов, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, John.1.9.98@mail.ru*

УДК 34.06

Аннотация. **С 2018 г. в силу вступил Федеральный закон** №187-ФЗ, предназначенный для регулирования отношений в области обеспечения безопасности объектов информационной инфраструктуры РФ, что потребовало появления алгоритмов и методик, упрощающих процедуру оценивания значимости объектов КИИ. В работе приводится методика оценки политической значимости угроз объекту КИИ и применение представленной методики на объекте инфокоммуникаций. Целью исследования является разработка удобного средства для проведения категорирования объекта с точки зрения политической значимости.

Ключевые слова: информационная безопасность; модель; оценка; критическая информационная инфраструктура; политическая значимость; показатели.

METHODOLOGY FOR ASSESSING THE POLITICAL SIGNIFICANCE OF THREATS TO A CII OBJECT ON THE EXAMPLE OF AN INFOCOMMUNICATION OBJECT

Evgeny Smirnov, *Saint Petersburg state University of telecommunications named Prof. M.A. Bonch-Bruevich.*

Annotation. Since 2018, put into effect Federal law No. 187-FZ, intended to regulate relations in the field of ensuring the security of information infrastructure objects in the Russian Federation, which required the appearance of algorithms and techniques that simplify the procedure for evaluating the significance of CII objects. The research paper presents a method for assessing the political significance of threats to the object of CII, and the application of the presented method to the object of Infocommunications. The purpose of the study is to develop a convenient tool for categorizing an object in terms of political significance.

Keywords: information security; model; assessment; critical information infrastructure; political significance; parameter.

Введение

В наши дни почти все сферы жизни государства, общества и человека стали зависимыми от информационных инфраструктур. За исключением отдельных стран, мобильными телефонами владеют больше 60 процентов населения по всему миру, а регулярно пользуются интернетом и социальными сетями более половины населения планеты. Касательно России, согласно прогнозам аналитиков, в 2020-2025 гг. будет наблюдаться стремительный темп увеличения российской интернет-аудитории вплоть до 80 млн человек, что составляет более 70% от населения страны. Такие высокие показатели означают, что информационная инфраструктура является крайне востребованной, а значит, тема информационной безопасности является актуальной как на мировом уровне, так и внутри страны. Чаще всего кибератакам подвергаются объекты критической информационной инфраструктуры (КИИ): информационные системы, автоматизированные системы

управления, информационно-телекоммуникационные системы, государственные учреждения и компании, которые функционируют во всех областях жизнеобеспечения городов, субъектов и всей страны [1].

Стоит сделать акцент на том, что объекты критической информационной инфраструктуры требуют уголовно-правовой охраны, поэтому решение о введении в уголовный кодекс соответствующих статей, направленных на привлечение к уголовной ответственности лиц, посягающих на объекты информационной инфраструктуры особой значимости, обосновано [2].

Основные понятия КИИ

Начало работ по защите информационной инфраструктуры в государственном масштабе было положено с подписанием Указа Президента Российской Федерации от 15 января 2013 г. № 31 с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Далее, в июле 2017 г. был подписан Федеральный Закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 №187-ФЗ[1] . Закон вступил в силу 1 января 2018 г. и вызвал необходимость проведения процедуры категорирования у множества объектов, что автоматически поставило вопрос оценки угроз объектам критической информационной инфраструктуры особенно остро.

Для понимания важнейших моментов в вопросе оценки значимости объектам КИИ следует разобраться с основными понятиями закона № 187-ФЗ[2].

Критическая информационная инфраструктура − объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Законодательно обозначено, что любые компьютерные системы или сети, принадлежащие субъектам категории «субъект критической информационной инфраструктуры», являются объектом критической информационной инфраструктуры.

Объекты критической информационной инфраструктуры − информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

Субъекты критической информационной инфраструктуры − государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы (ИС), информационно-телекоммуникационные сети (ИТС), автоматизированные системы управления (АСУ), функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или)

[1] Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

[2] Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ.

индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [3].

Принимая во внимание эти определения, несложно понять, что такое КИИ, что является «объектом КИИ», а что «субъектом», и в каких именно отраслях они функционируют. Становится ясно, что все информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъекта КИИ − это объекты КИИ.

Важно отметить, что большинство субъектов КИИ на момент принятия закона № 187-ФЗ уже имели в наличии некоторые механизмы безопасности, а значит, что объекты категорирования не нуждаются в полном создании, а могут потребовать лишь некоторой доработки и соответствующего документирования.

Категорирование субъектов требуется, если они подпадают хотя бы под один критерий значимости объектов КИИ, которые условно могут быть сгруппированы в пять направлений:

1. Социальная значимость.
2. Политическая значимость.
3. Экономическая значимость.
4. Экологическая значимость.
5. Значимость для обеспечения обороны страны, безопасности государства и правопорядка [4].

Содержание методики оценки политической значимости угроз объекту КИИ

Рассмотрим методику оценки политической значимости угроз объекту КИИ применительно к объекту телекоммуникаций − университету телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ):

1. Формирование комиссии.

Для категорирования объектов КИИ формируется экспертная комиссия. В общем случае в ее состав входят: руководитель субъекта КИИ / уполномоченное им лицо, участвующие в процессах специалисты, специалисты по информационной безопасности, специалисты по защите государственной тайны, работники в области гражданской обороны (ГО) и чрезвычайных ситуаций (ЧС). Комиссия является постоянно действующей до момента ее расформирования, которое производится в случаях ликвидации субъекта или прекращения выполнения им своих полномочий в определенных направлениях. Комиссия может быть создана отдельно для филиалов или представительств организации.

Для вуза подобная комиссия будет состоять из ректора или уполномоченного им лица, специалистов Федеральной службы по надзору в сфере образования и науки, специалистов промышленной безопасности, специалистов отдела АСУ ТП, специалистов отдела информационных технологий, ответственных за обеспечение безопасности в АСУ ТП, работников подразделения по защите государственной тайны, специалистов по промышленной безопасности, по гражданской обороне и защите от чрезвычайных ситуаций.

2. Определение принадлежности организации к субъектам КИИ.

Для того чтобы определить, является ли рассматриваемая организация субъектом КИИ, следует обратиться к постановлению 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». В документе приведена таблица перечня показателей критериев значимости, и в случае, если вид деятельности анализируемой организации подпадает под приведенные в постановлении процессы – она является субъектом КИИ [5].

Является ли университет телекоммуникаций субъектом КИИ? Каждый вуз может попасть под законодательство о критической информационной инфраструктуре, поскольку любой из них является социальной структурой. В обозначенной выше таблице, одним из показателей критериев социальной значимости является отсутствие доступа к государственной услуге, чем и является образовательный процесс. Поэтому университет телекоммуникаций является объектом КИИ, к тому же, помимо социальной, он содержит такие критерии значимости как политическая (будет рассмотрена далее), экологическая (включает в себя кафедру экологической безопасности телекоммуникации и производит обучение по этому направлению [6]), значимость для обеспечения обороны страны, безопасности государства и правопорядка (содержит военную кафедру, а также военно-учетный стол [7]).

3. Определение всех критических процессов рассматриваемой организации, связанных с политической значимостью.

Под политической значимостью подразумеваются два показателя, первым из них является прекращение или нарушение функционирования государственного органа в части невыполнения возложенных на него функций (полномочий). Существуют три категории для его значимости:

- III категория − это прекращение или нарушение функционирования органа государственной власти субъекта Российской Федерации или города федерального значения;
- II категория − это прекращение или нарушение функционирования федерального органа государственной власти;
- I категория − это прекращение или нарушение функционирования Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации.

Вторым показателем является нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации. Для этого показателя также существуют три значения категорий:

- III категория − это нарушение условий договора межведомственного характера (срыв переговоров или подписания);
- II категория − это нарушение условий межправительственного договора (срыв переговоров или подписания);
- I категория − это нарушение условий межгосударственного договора (срыв переговоров или подписания).

Для категорий значимости самой высокой является первая категория, а самой низкой – третья, потенциальный ущерб учитывается по охваченной территории и по количеству пострадавших людей.

В рамках деятельности организации процессы оказывают разное влияние на результат ее деятельности, поэтому необходимо выделять те процессы, которые оказывают наибольшее воздействие на достижение главных целей, именно они и являются критическими.

Для их выявления изучают информационные ресурсы (файлы и базы данных), программные ресурсы (системное и прикладное ПО) и технические ресурсы (коммутационное оборудование, компьютеры, серверы), выделяют основные процессы деятельности субъектов КИИ (управленческие, технологические, производственные, финансово-экономические и др.).

Выявлением всех критических процессов занимается экспертная комиссия. Примерами критических процессов политической значимости университета могут служить: обучение студентов по обмену, проведение международных конференций, сотрудничество с крупнейшими инфокоммуникационными компаниями. Все перечисленные процессы несут в себе политическое содержание, поскольку для их исполнения заключаются соглашения о сотрудничестве и межведомственные договоры. Поскольку вуз является государственным, то нарушения условий с его стороны могут повлечь за собой различные негативные последствия, которые могут отразиться на политической ситуации как внутри, так и за пределами страны.

4. Выделение объектов, связанных с рассмотренными критическими процессами.

На данном этапе выделяются подразделения и системы, в которых осуществляется управление, контроль или мониторинг критических процессов, обрабатывается информация, необходимая для обеспечения выполнения критических процессов, а также осуществляется поиск потенциальных уязвимостей и угроз безопасности, которыми может воспользоваться нарушитель.

В рассматриваемом примере объектами, осуществляющими управление, контроль и мониторинг являются отдел международного сотрудничества, отдел по работе с предприятиями, а также подразделения Проректора [8]. Для более полного отображения информации о том, как связаны объекты и процессы, рекомендуется составить табл. 1.

Таблица 1.

№	Процесс	Функции объекта КИИ			
		Обработка	**Управление**	**Контроль**	**Мониторинг**
1	Обучение студентов по обмену	Отдел международного сотрудничества	Отдел международного сотрудничества	Подразделение проректора по учебной работе	Отдел международного сотрудничества
2	Проведение международных конференций	Отдел международного сотрудничества	Отдел международного сотрудничества	Подразделение проректора по научной работе	Отдел международного сотрудничества
3	Сотрудничество с компаниями отрасли телекоммуникации	Отдел по работе с предприятиями	Отдел по работе с предприятиями	Подразделение проректора по развитию	Отдел по работе с предприятиями

Максимальный срок категорирования, в соответствии с требованиями законодательства, не должен превышать одного года с момента утверждения Перечня объектов КИИ (внесения изменений, дополнений).

5. Оценка критериев значимости.

Оценка критериев значимости производится на основе постановления Правительства № 127. Чем более значительными могут быть последствия, тем категория выше, и наоборот. Под первую категорию подпадают нарушение условий межгосударственного договора или прекращение функционирования органов верховной государственной власти Российской Федерации. Под вторую – прекращение деятельности федерального органа или срыв межправительственного договора. И под третью категорию подпадает остановка функционирования субъекта РФ или города федерального значения или нарушение договора межведомственного характера.

Рассмотренные в примере критические процессы производятся в рамках международного сотрудничества, но между ведомствами стран. Это означает, что рассмотренные процессы при их неудачном развитии могут привести к нарушению условий межведомственного договора, то есть подпадать под третью категорию критерия политической значимости постановления Правительства № 127.

6. Подготовка необходимых документов для категорирования объектов КИИ.

По результатам выполнения всех предыдущих пунктов у комиссии собраны, систематизированы и оценены данные по всем критическим процессам и объектам, которые с ними связаны. Базируясь на этом, оформляется акт категорирования субъекта КИИ. Документ подписывается членами комиссии по категорированию и утверждается руководителем субъекта критической информационной инфраструктуры и хранится до вывода из эксплуатации объекта критической информационной инфраструктуры или до изменения его категории значимости. Информация о присвоении объекту КИИ одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий, должна быть отправлена во ФСТЭК России в течение 10 дней со дня утверждения акта. Пересмотр установленной категории значимости должен выполняться не реже чем раз в пять лет [9].

Акт категорирования не имеет стандартной формы, хранится как документ внутреннего пользования, и может быть запрошен при проверке объекта. В акте категорирования должна быть отражена следующая информация:

- Сведения о присвоенной объекту КИИ категории значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий.
- Сведения об объекте КИИ.
- Результаты анализа угроз информационной безопасности объекта КИИ.
- Реализованные меры по обеспечению безопасности объекта КИИ.
- Сведения о необходимых мерах по обеспечению безопасности [10].

Объект информационной инфраструктуры может быть отнесен к критическому только после внесения его в реестр значимых объектов критической информационной инфраструктуры (ст. 8 № 187-ФЗ).

Заключение

С началом действия федерального закона № 187 субъекты, на которые распространяются нормы данного закона, должны организовать целый комплекс

мероприятий по соблюдению положений данного нормативного акта. При этом, некоторые рассматриваемые субъекты и объекты, которые необходимо категорировать в соответствии с новыми постановлениями, уже прошли соответствующую классификацию до вступления в силу 187-ФЗ, и, как правило, уже имеют соответствующую систему обеспечения безопасности и систему защиты информации. Следовательно, для большинства предприятий, учреждений и организаций, задача категорирования и обеспечения безопасности сводится к модернизации защиты информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления под установленные требования, а также их документирование [11].

Предложенная методика оценки политической значимости угроз объекту КИИ призвана облегчить работу в этом направлении. Для большей демонстративности она была применена на объекте инфокоммуникаций − университете телекоммуникаций им. проф. М.А. Бонч-Бруевича. Дополнительно при использовании методики, применительно к другим объектам, может помочь составление модели угроз, модели нарушителей, а также использование статистики по инцидентам [12].

Литература

1. Ермилов Е.В., Калашников А.О., Чопоров О.Н., Разинкин К.А., Баранников Н. И., Корнеева Н. Н. Управление информационными рисками при атаках на АСУ ТП критически важных объектов: учеб. пособие. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2013. – 109 с.
2. Дремлюга Р.И., Зотов С.С., Павлинская В..Ю. Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-тихоокеанский регион: Экономика, политика, право, 2019. – Т. 21. – №. 2. – С. 130-139.
3. Алейникова О.В., Базарова А.А., Цап Т.В. Требования безопасности объектов критической информационной инфраструктуры и этапы их реализации // Информационные технологии и системы: управление, экономика, транспорт, право, 2019. – № 3. – С. 70-76.
4. Шумский И. Н. Управление информационной безопасностью предприятия в части категорирования КИИ и анализа модели угроз: дис. – Сибирский федеральный университет; Хакасский технический институт − филиал СФУ, 2019.
5. Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 13.04.2019) "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".
6. Сайт кафедры экологической безопасности телекоммуникации [Электронный ресурс]. – Режим доступа: https://www.sut.ru/index.php/teaching/ft/rstvmt/kaf-ebgd (дата обращения: 29.04.2020).
7. Второй отдел [Электронный ресурс]. – Режим доступа: https://www.sut.ru/home/hide/vtoroj-otdel (дата обращения: 29.04.2020);
8. Структура и органы управления образовательной организацией [Электронный ресурс]. – Режим доступа: https://www.sut.ru/sveden/struct (дата обращения: 29.04.2020).
9. Категорирование объектов критической информационной инфраструктуры (КИИ). Практические примеры [Электронный ресурс]. – Режим доступа: https://rtmtech.ru/articles/kategorirovanie-obektov-kii-primery/ (дата обращения: 29.04.2020).

10. Шабуров А.С., Двойнишников Н.Э. Особенности реализации требований по категорированию объектов критической информационной инфраструктуры // Вестник УрФО. Безопасность в информационной сфере, 2018. – №. 4 (30). – С. 75-82.
11. Щелкин К.Е., Звягинцева П.А., Селифанов В.В. Возможные подходы к категорированию объектов критической информационной инфраструктуры // Интерэкспо Гео-Сибирь, 2019. – Т. 6. – №. 1.
12. Новикова Е.Ф., Хализев В.Н. Разработка модели угроз для объектов критической информационной инфраструктуры с учетом методов социальной инженерии // Прикаспийский журнал: управление и высокие технологии, 2019. – № 4. – С. 127-135.