ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
2023. Т. 5, № 5 (14). С. 78–87 http://siit.ugatu.su
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056 DOI 10.54708/2658-5014-SIIT-2023-no5-p78

Управление рисками нарушения информационной безопасности значимых объектов критической информационной инфраструктуры

М. А. Бакулин

Аннотация. Статья посвящена анализу и практической реализации этапов управления рисками информационной безопасности критической информационной инфраструктуры (КИИ). Описывается процесс предпроектного анализа объекта исследования, выделения объектов КИИ и их категорирования, оценки рисков с использованием нечетких когнитивных карт и их снижения в соответствии с требованиями нормативно-правовой базы, которые предъявляется к значимым объектам КИИ. Снижение рисков нарушения информационной безопасности реализуется за счет модернизации системы защиты информации и реорганизации сети. Рассматриваются возможные варианты обработки риска.

Ключевые слова: защита информации; информационная безопасность; критическая информационная инфраструктура; система защиты информации; риски нарушения информационной безопасности, нечеткие когнитивные карты.

Введение

Текущая стадия развития мировой экономики связана с цифровизацией практически всей промышленности и большинства сфер человеческой жизни [1]. В настоящее время сложно представить деятельность какой-либо организации без использования информационных систем (ИС), информационно-телекоммуникационных сетей (ИТС) и/или автоматизированных систем управления технологическими процессами (АСУ ТП). Они в свою очередь являются объектами критической информационной инфраструктуры (КИИ), если принадлежат субъекту КИИ или же если субъект КИИ обеспечивает их взаимодействие. Также стоит выделить сложные распределенные системы, которые базируются на использовании ИС [2]. Субъектом КИИ в свою очередь может быть государственный орган, государственное учреждение, юридическое лицо или индивидуальный предприниматель (ИП), которые функционируют в одной из 13 отраслей: оборонная промышленность, энергетика, финансовая сфера, здравоохранение, атомная энергетика и т. д. Данные отрасли и другие основополагающие аспекты обеспечения безопасности КИИ изложены в Федеральном законе № 187[1].

За последние несколько лет все больше внимания стало уделяться обеспечению безопасности КИИ. И обеспечение такой безопасности стало приоритетной государственной задачей [3]. Это вызвано тем, что количество таргетированных атак на значимые объекты КИИ РФ с каждым годом растет. Согласно информации от компании Positive Technologies, количество атак в первом полугодии 2021 г. на объекты КИИ выросло более чем в 2 раза относительно года ранее, и при этом около 60% из них были реализованы при поддержке того или иного государства [4]. Интенсивность этих атак продолжает расти по сей день. Кроме того, популярность глубокого внедрения промышленного Интернета вещей в критическую инфраструктуру достаточно сильно увеличивает масштабы последствий от проведения в отношении них компьютерных атак [5]. Например, такой тип атак, как «degradation-of-QoS attack», целями которых являются VANET сети [6]. Наибольшая уязвимость в КИИ вносится за счет операционных систем, общедоступных протоколов передачи данных типа TCP/IP и разнообразных сетевых

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

сервисов [7]. Требования по обеспечению безопасности таких объектов ужесточаются, выпускаются и уточняются соответствующие нормативно-правовые акты (НПА) [8], а внимание регуляторов только увеличивается. За несоблюдение предъявляемых к КИИ требований предъявляется соответствующая ответственность вплоть до уголовной [9]. Соответственно субъектам КИИ необходимо выполнять предъявляемые к ним требования по обеспечению безопасности, которые закреплены в соответствующих приказах и постановлениях. Конечной целью данных требований является обеспечение и поддержание необходимого уровня защищенности значимых объектов КИИ или допустимого уровня риска нарушения информационной безопасности (ИБ). Формулировка зависит от того понятийного аппарата, которого придерживаются в организации, ведь смысл в обоих случаях одинаков, то есть конечная цель – это обеспечение устойчивого функционирования значимых объектов КИИ при проведении в отношении них компьютерных атак. Данный процесс является циклическим [10]. Таким образом, согласно необходимости внедрения риск-ориентированного подхода, существует потребность в непосредственной оценке риска [11]. Несмотря на стремительное развитие НПА, в области КИИ отмечаются также ряд недостатков в текущих документах, которые требуют совершенствования [12].

Подготовка к оценке

Данный этап заключается в сборе исходной информации об объекте исследования, которая будет использоваться в дальнейших стадиях управления рисками нарушения ИБ [13]. Сначала необходимо определить вид деятельности рассматриваемой организации для выяснения типа информационной системы (КИИ, ИСПДн, АСУ ТП, ГИС), что позволит определить группу стандартов, которых данной организации необходимо придерживаться. В качестве объекта исследования в данной работе рассматривается одна из крупных стоматологических поликлиник. Данная организация является государственной и в соответствии с ее лицензией, которая выдана Министерством здравоохранения РФ на осуществление медицинской деятельности, и уставом организации – она осуществляет деятельность в сфере здравоохранения. Следовательно, данный субъект относится к КИИ. Локально-вычислительная сеть (ЛВС) данной организации представлена на рисунке 1.

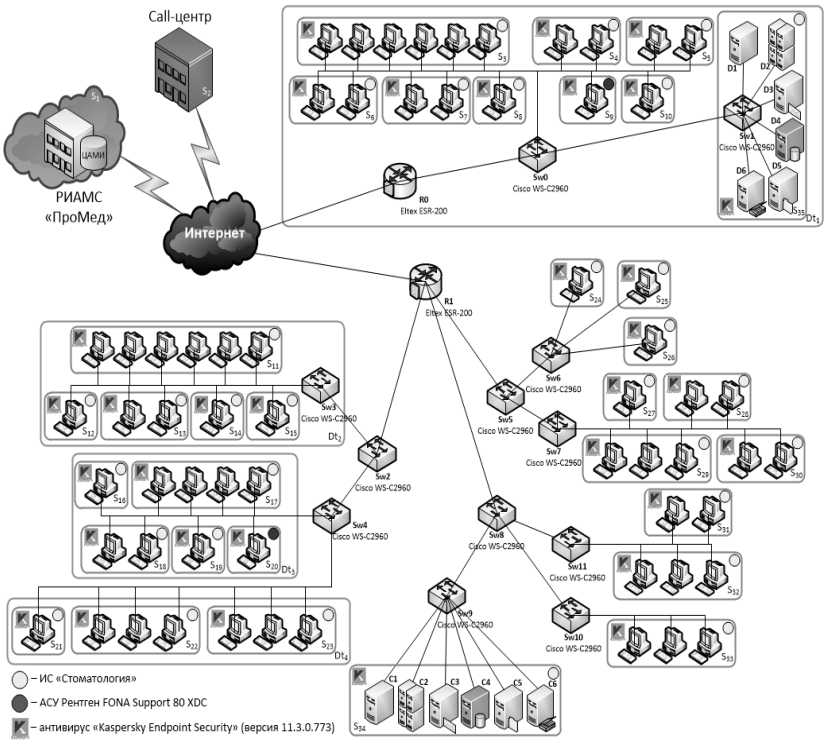

Рис. 1 Топология сети.

После этого необходимо выделить объекты КИИ и провести их категорирование. Для этого необходимо составить перечень всех имеющихся активов и определить место их хранения в соответствии с топологией сети. Для исследуемого объекта фрагмент перечня активов представлен в таблице 1.

Далее необходимо выделить бизнес-процессы. Фрагмент перечня бизнес-процессов исследуемого объекта представлен в таблице 2.

Таблица 1

Фрагмент перечня активов и их расположение

Актив	Место хранения
Штатное расписание Сведения о сотрудниках … Журнал учета материальных средств и стоматологической аппаратуры	D_1, D_5, C_1, C_5
Учет оказанных платных стоматологических услуг … Документы на поставку нового оборудования, медикаментов и предметов мебели	$S_{27–30}$
Графическое представление зубной формулы … Учет эстетических конструкций (виниры, композиты и т. п.)	D_2, C_2
Обращения пациентов … Корпоративные письма	D_3, C_3
Рентгеновские стоматологические снимки … Коды обследований рентгенографии	D_4, C_4

Таблица 2

Фрагмент перечня протекающих бизнес-процессов

Бизнес-процесс	Обозначение связи
Запись на прием в регистратуре (офлайн), с помощью приложения и по телефону	1
Уведомление пациентов о записи на прием	2
Направление на рентген ротовой полости	3
Оказание лечебных стоматологических услуг	4
Оказание услуг санации полости рта	5
Оказание услуг ортодонта	6
Оказание услуг стоматологического хирурга	7
Снятие рентгеновского снимка	8
Изготовление зубных имплантов, протезов и эстетических конструкций	9
Оказание услуг по лечению и профилактике околозубных тканей	10
…	…
Оплата платных стоматологических услуг	18
Разработка политики управления стоматологией, плановых и отчетных форм	19
Оформление отчетов о движении денежных средств	20
Ведение списка сотрудников	21
Руководство над отделениями и контроль выполнения планов	22
Обеспечение работы оборудования и вычислительной техники	23
Списание стоматологического оборудования, техники и мебели	24

Также необходимо описать процесс протекания бизнес-процессов в соответствии с топологией сети и сформировать модель. Результат построения такой модели представлен на рисунке 2.

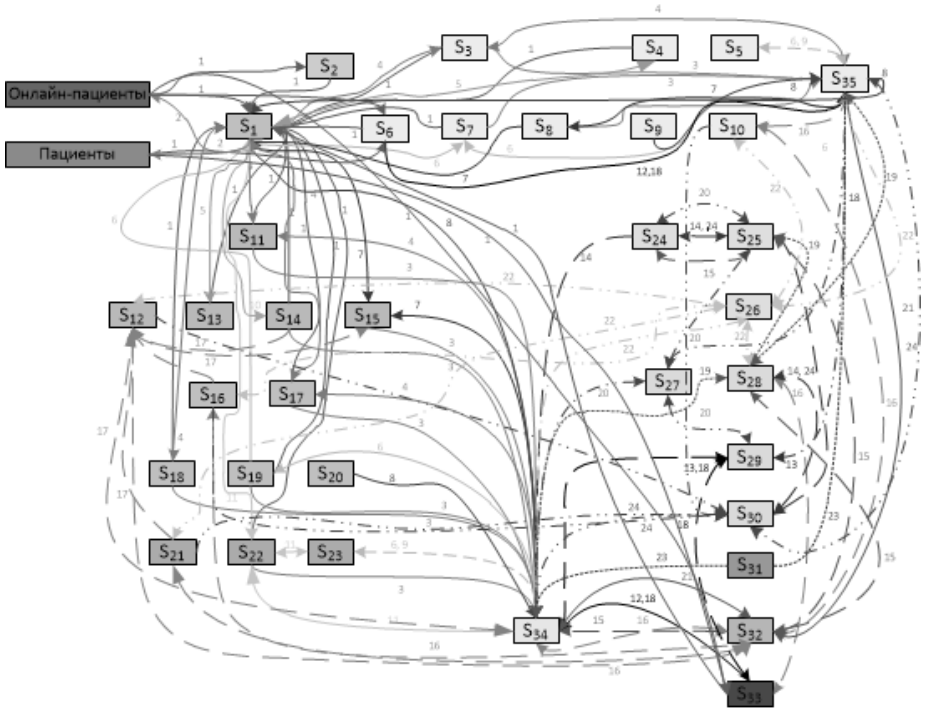

Рис. 2 Модель протекания бизнес-процессов.

После определения всех бизнес-процессов необходимо выделить из них критичные, а также выяснить, какие объекты (АСУ, ИС и/или ИТС) обеспечивают их функционирование. Данные объекты и будут являться объектами КИИ. Критические процессы и объекты КИИ представлены в таблице 3.

Таблица 3

Критические бизнес-процессы и объекты

№ п/п	Объект КИИ	Тип объекта	Обеспечиваемый критический процесс
1	Рентген FONA Support 80 XDC	АСУ	3, 8
2	ИС «Стоматология»	ИС	3, 4, 6, 7, 8, 11, 13, 17, 18, 23
3	ЛВС организации	ИТС	1, 3, 4, 5, 6, 7, 8, 10, 11, 13, 17, 18, 23

После выявления объектов КИИ необходимо провести их категорирование в соответствии с Постановлением Правительства РФ № 127[2]. В результате категорирования всем трем объектам КИИ была присвоена 3-я категория значимости.

После категорирования объектов КИИ необходимо провести анализ текущей системы защиты информации (СЗИ) и выявить те средства защиты информации (СрЗИ), которые нужно заменить, добавить и/или исключить в соответствии с предъявляемыми мерами обеспечения безопасности, согласно приказу ФСТЭК № 239[3]. В соответствии с данным приказом был опре-

[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 от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

делен и адаптирован перечень мер защиты, которые должны быть реализованы для 3-й категории значимости. Перечень функциональных подсистем защиты для реализации предъявляемых мер защиты представлен в таблице 4.

Таблица 4

Необходимые функциональные подсистемы СрЗИ

Подсистемы СрЗИ	Причина внедрения/замены
МЭ	Замена по причине отсутствия у имеющихся МЭ действующих сертификатов
СЗИ от НСД	Внедрение по причине отсутствия
СКЗИ	Замена по причине отсутствия у имеющихся СКЗИ действующих сертификатов
СДЗ	Внедрение по причине отсутствия
Сканер безопасности сети	Внедрение по причине отсутствия

Оценка риска нарушения ИБ

На сегодняшний день нет какого-либо нормативно закрепленного метода или программного продукта для оценки риска нарушения ИБ. Организация сама решает, какой метод или программный продукт она будет использовать. Существуют как качественные, так и количественные методы оценки риска. В данной работе проведена количественная оценка риска нарушения ИБ с использованием нечетких когнитивных карт (НКК) [14]. Связи между концептами НКК имеют веса в соответствии с актуальными уязвимостями (максимальными). Сформированная НКК до модернизации СЗИ и реорганизации сети представлена на рисунке 3.

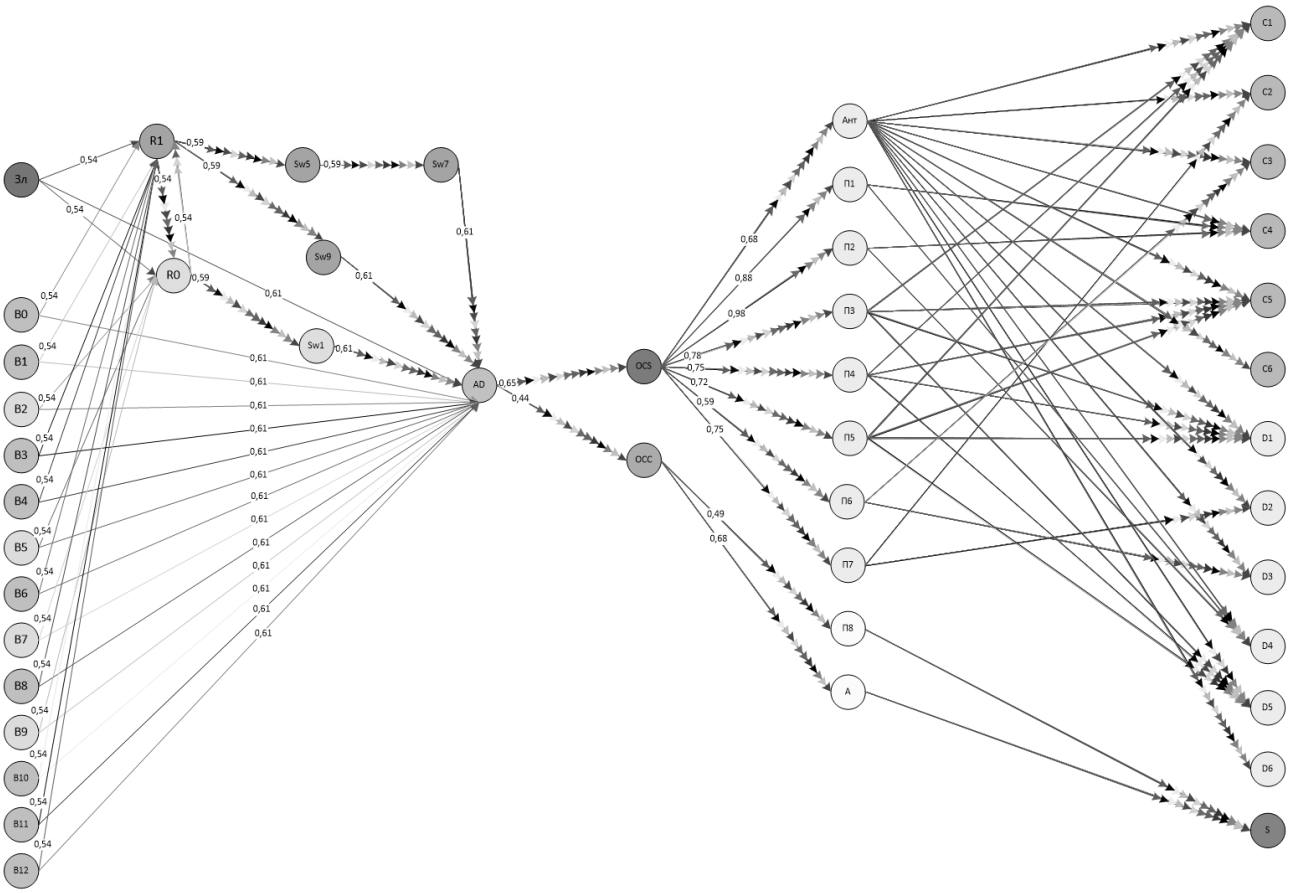

Рис. 3 НКК до модернизации СЗИ и реорганизации сети.

После моделирования была определена ценность каждого объекта атаки. В соответствии с данной НКК были вычислены результирующий уровень угроз и уровень риска как для каждого объекта атаки, так и итоговое значение риска (таблица 5) [15].

Таблица 5

Результирующие уровни угроз, уровни риска

Объекты атаки		Результирующий уровень угроз	Уровень риска
Сегмент	Ценность		
$S_{27\text{-}30}$	0.2	0.128499163	0.0257
D_1	0.06	0.177827441	0.0107
D_2	0.05	0.130356485	0.0065
D_3	0.055	0.539781199	0.0297
D_4	0.085	0.098760615	0.0084
D_5	0.055	0.247249999	0.0136
D_6	0.045	0.160500355	0.0072
C1	0.085	0.214809606	0.0183
C2	0.056	0.246252081	0.0138
C3	0.07	0.539781199	0.0378
C4	0.094	0.129612877	0.0122
C5	0.085	0.441611512	0.0375
C6	0.06	0.189883483	0.0114
		Итог	0.2327

В результате оценки изначальный риск нарушения ИБ составил 23.27%.

Обработка риска нарушения ИБ

Варианты обработки риска могут быть следующие: снижение риска; сохранение риска; предотвращение риска; перенос риска. В данном случае значение риска является недопустимым, а экономическая целесообразность его снижения оправдана. Риски необходимо снижать за счет модернизации СЗИ в соответствии с НПА, которые предъявляются к данным объектам КИИ. Также в данной работе риск был снижен за счет реорганизации ЛВС, поскольку в исходной сети были нарушения ее сегментирования, а именно – общедоступные серверы не были выведены в демилитаризованную зону (DMZ). Топология сети после модернизации СЗИ и реорганизации сети представлена на рисунке 4.

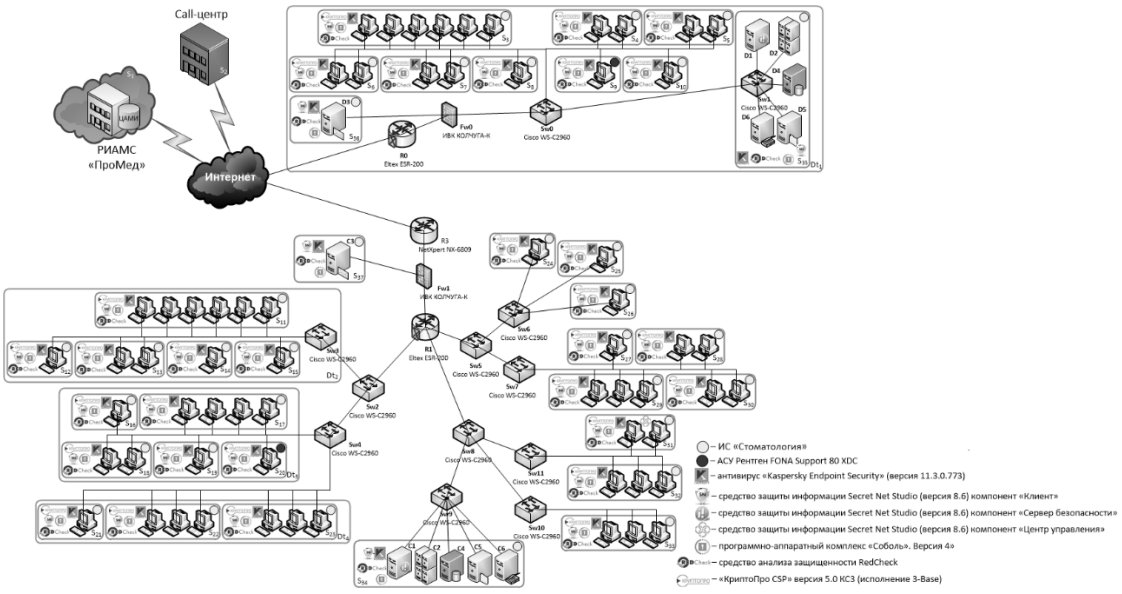

Рис. 4 Топология сети после реорганизации с учетом модернизации СЗИ.

Оценка остаточного риска нарушения ИБ

После модернизации СЗИ и реорганизации сети необходимо внести соответствующие изменения в НКК, а именно – добавить, заменить и/или убрать соответствующие концепты и связи, веса которых соответствуют добавляемым средствам и программным продуктам. Результаты изменений представлены на рисунке 5.

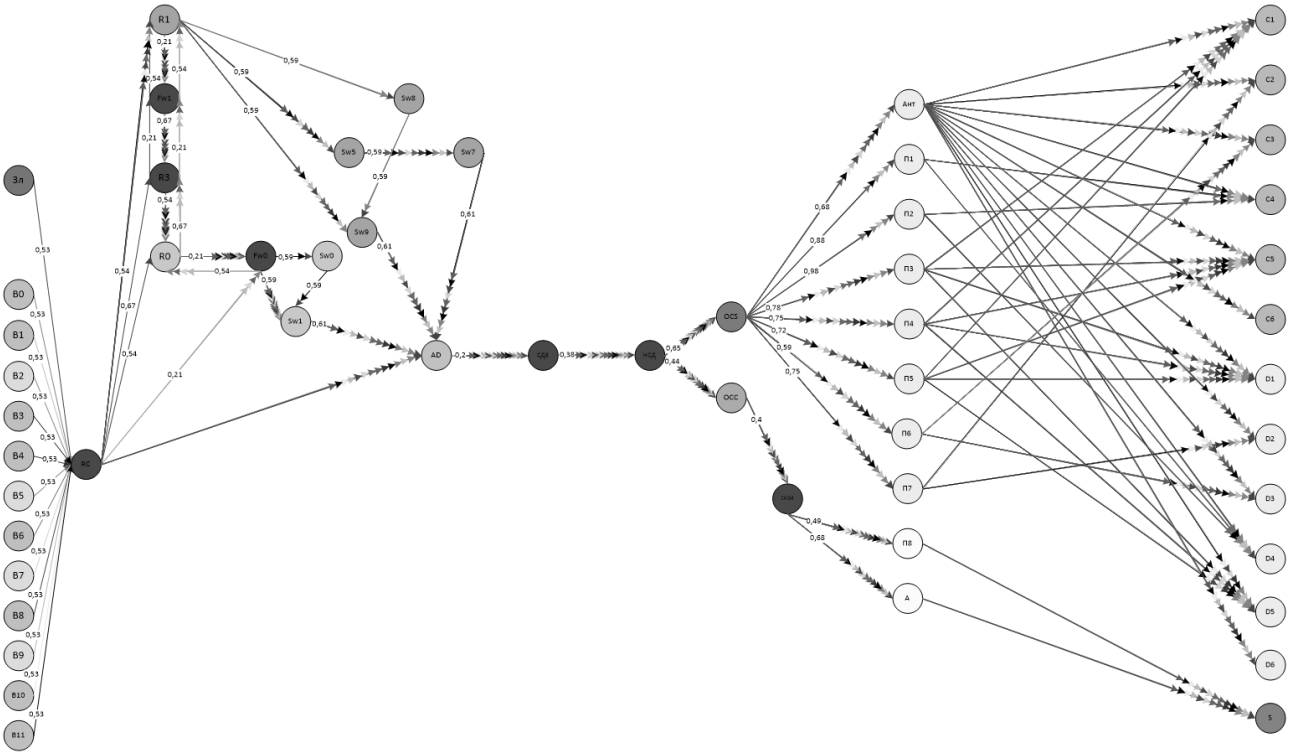

Рис. 5 НКК после реорганизации сети с учетом модернизации СЗИ.

После того как все действия предпринятые для снижения значения риска нарушения ИБ были учтены и отражены в НКК, необходимо провести соответствующие вычисления, которые аналогичны проводимым вычислениям ранее. Результаты вычислений и итоговое значение риска представлены в таблице 6.

Таблица 6

Результирующие уровни угроз, уровни риска

Объекты атаки		Результирующий уровень угроз	Уровень риска
Сегмент	Ценность		
$S_{27\text{-}30}$	0.2	0.020357899	0.0041
D_1	0.06	0.016239231	0.0010
D_2	0.05	0.010063567	0.0005
D_3	0.055	0.194503484	0.0107
D_4	0.085	0.007459359	0.0006
D_5	0.055	0.057873049	0.0032
D6	0.045	0.01428174	0.0006
C1	0.085	0.051911416	0.0044
C2	0.056	0.061582603	0.0034
C3	0.07	0.194503484	0.0136
C4	0.094	0.029496123	0.0028
C5	0.085	0.139144235	0.0118
C6	0.06	0.04539445	0.0027
Итог			0.0595

Решение по остаточному риску

В результате обработки риска его значение стало равно 5.95%. Данное значение является допустимым в соответствии с политикой безопасности, принятой в организации, а дальнейшее его снижение экономически нецелесообразно (материальные средства на дальнейшее его снижение больше тех средств, которые могут быть утрачены в результате ущерба в случае успешной реализации той или иной угрозы).

Заключение

В данной статье представлены этапы, которые включает в себя процесс управления рисками нарушения ИБ: подготовка к оценке риска, оценка риска, первичная обработка риска, оценка остаточного риска и решение по остаточному риску.

Данные этапы были реализованы в рамках рассмотрения стоматологической поликлиники в качестве субъекта КИИ. Были выявлены активы и место их хранения в соответствии с топологией сети, бизнес-процессы и модель их протекания, выявлены критические процессы и объекты, которые обеспечивают их функционирование. В результате категорирования всем трем объектам была присвоена 3 категория значимости. Был рассчитан исходный риск нарушения ИБ, он составил 23.27%. Данный риск был недопустим, в результате чего был снижен до 5.95%, то есть в 3.91 раза за счет модернизации СЗИ в соответствии с требованиями НПА, а также за счет реорганизации сети. Поскольку данное значение риска является допустимым и экономически обоснованным, то на этом процесс управления рисками был завершен.

Благодарности

Автор выражает признательность научному руководителю канд. техн. наук Алине Юрьевне Сенцовой за постановку задач в рамках данного исследования и консультационную помощь по теме исследования.

Список литературы / References

1. Васильев В. И., Картак В. М. Применение методов искусственного интеллекта в задачах защиты информации (по материалам научной школы УГАТУ) // Системная инженерия и информационные технологии. 2020. Т. 2. № 2 (4). С. 43–50. [[Vasilyev V. I., Kartak V. M. “Application of artificial intelligence methods in information security problems (based on materials from the scientific school of UGATU)” // System Engineering and Information Technologies. 2020. Vol. 2, No. 2 (4), pp. 43-50. (In Russian).]]

2. Закирова Э. Ф., Павлов С. В., Трубин В. Д., Христодуло О. И. Детализация пространственной информации для обеспечения защищенности баз данных в распределенных информационных системах // Системная инженерия и информационные технологии. 2022. Т. 4. № 1 (8). С. 20–26. [[Zakirova E. F., Pavlov S. V., Trubin V. D., Christodoulo O. I. “Detailing spatial information to ensure the security of databases in distributed information systems” // System Engineering and Information Technologies. 2022. Vol. 4, No. 1 (8), pp. 20-26. (In Russian).]]

3. Горбатов В. С., Жуков И. Ю., Кравченко В. В., Правиков Д. И. Кибербезопасность сетевого периметра объекта критической информационной инфраструктуры // Безопасность информационных технологий. 2022. Т. 28. № 4. [[Gorbatov V. S., Zhukov I. Yu., Kravchenko V. V., Pravikov D. I. “Cybersecurity of the network perimeter of a critical information infrastructure facility” // Security of Information Technologies. 2022. Vol. 28. No. 4. (In Russian).]]

4. Российские объекты КИИ [Электронный ресурс]. URL: https://www.comnews.ru/content/215455/2021-07-14/2021-w28/rossiyskie-obekty-kii-podverglis-usilennym-atakam (дата обращения: 05.03.2023). [[Russian Objects of KII [Electronic resource]. URL: https://www.comnews.ru/content/215455/2021-07-14/2021-w28/rossiyskie-obekty-kii-podverglis-usilennym-atakam (access date: 03/05/2023). (In Russian).]]

5. Вульфин А. М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных // Системная инженерия и информационные технологии. 2023. Т. 5. № 4 (13). [[Vulfin A. M. “Models and methods for comprehensive assessment of security risks of objects of critical information infrastructure based on intelligent data analysis” // System Engineering and Information Technologies. 2023. Vol. 5, No. 4 (13). (In Russian).]]

6. Легашев Л. В., Парфенов Д. И., Болодурина И. П., Ушаков Ю. А. Вопросы безопасности сервисов в самоорганизующихся сетях интеллектуальной транспортной системы VANET // Системная инженерия и информационные технологии. 2020. Т. 2. № 2 (4). С. 36–42. [[Legashev L. V., Parfenov D. I., Bolodurina I. P., Ushakov Yu. A. “Issues of security of services in self-organizing networks of the intelligent transport system VANET” // System Engineering and Information Technologies. 2020. Vol. 2. No. 2 (4), pp. 36-42. (In Russian).]]

7. Климов С. М., Поликарпов С. В., Рыжов Б. С., Тихонов Р. И., Шпырня И. В. Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий // Вопросы кибербезопасности. 2019. № 6 (34). [[Klimov S. M., Polikarpov S. V., Ryzhov B. S., Tikhonov R. I., Shpyrnya I. V. “Methodology for ensuring the sustainability of the functioning of critical information infrastructure under conditions of information impacts” // Issues of Cybersecurity. 2019. No. 6 (34). (In Russian).]]

8. Горелик В. Ю., Безус М. Ю. О безопасности критической информационной инфраструктуры Российской Федерации // StudNet. 2020. № 9. [[Gorelik V. Yu., Bezus M. Yu. “On the security of the critical information infrastructure of the Russian Federation” // StudNet. 2020. No. 9. (In Russian).]]

9. Трунцевский Ю. В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. [[Truntsevsky Yu. V. “Unlawful influence on critical information infrastructure: criminal liability of its owners and operators” // Journal of Russian Law. 2019. No. 5. (In Russian).]]

10. Гавдан Г. П., Иваненко В. Г., Рыбалко Э. П., Рыбалко Д. П. Устойчивость функционирования объектов критической информационной инфраструктуры // Безопасность информационных технологий. 2022. Т. 29. № 4. [[Gavdan G. P., Ivanenko V. G., Rybalko E. P., Rybalko D. P. Stability of the functioning of critical information infrastructure objects // Security of Information Technologies. 2022. Vol. 29. No. 4. (In Russian).]]

11. Кочергин Г. А., Муратов И. Н., Куприянов М. А. Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий // Вопросы кибербезопасности. 2019. № 6 (34). [[Kochergin G. A., Muratov I. N., Kupriyanov M. A. “Methodology for ensuring the sustainability of the functioning of critical information infrastructure under conditions of information influences” // Issues of Cybersecurity. 2019. No. 6 (34). (In Russian).]]

12. Наталичев Р. В., Горбатов В. С., Гавдан Г. П., Дураковский А. П. Эволюция и парадоксы нормативной базы обеспечения безопасности объектов критической информационной инфраструктуры // Безопасность информационных технологий. 2021. Т. 28. № 3. [[Natalichev R. V., Gorbatov V. S., Gavdan G. P., Durakovsky A. P. “Evolution and paradoxes of the regulatory framework for ensuring the safety of critical information infrastructure objects” // Security of Information Technologies. 2021. Vol. 28. No. 3. (In Russian).]]

13. Бакулин М. А. Управление рисками информационной безопасности в корпоративных информационных сетях // Мавлютовские чтения: Мат-лы XVI Всероссийской молодежной научной конференции. В 6 т. Уфа, 25–27 октября 2022 года. Т. 5. Уфа: Уфимский государственный авиационный технический университет, 2022. С. 482–490. [[Bakulin M. A. “Information security risk management in corporate information networks” // Mavlyutov’s readings: Materials of the XVI All-Russian Youth Scientific Conference. In 6 volumes, Ufa, October 25–27, 2022. Volume 5. Ufa: Ufa State Aviation Technical University, 2022. Pp. 482-490. (In Russian).]]

14. Бакулин М. А. Обеспечение защиты информации значимых объектов критической информационной инфраструктуры // Проблемы обеспечения безопасности (безопасность-2022): Мат-лы IV Международной научно-практической конференции, посвященной 90-летию УГАТУ, Уфа, 14 апреля 2022 года. Уфа: Уфимский государственный авиационный технический университет, 2022. С. 367–374. [[Bakulin M. A. “Ensuring the protection of information of significant objects of critical information infrastructure” // Problems of Ensuring Security (Security-2022): materials of the IV International scientific and practical conference dedicated to the 90th anniversary of UGATU, Ufa, April 14, 2022. Ufa: Ufa State Aviation Technical University, 2022. pp. 367-374. (In Russian).]]

15. Бакулин М. А. Анализ и повышение уровня защищенности значимого объекта критической информационной инфраструктуры // Мавлютовские чтения: Мат-лы XV Всероссийской молодежной научной конференции: в 7 томах, Уфа, 26–28 октября 2021 года. Т. 4. Уфа: Уфимский государственный авиационный технический университет, 2021. С. 331–342. [[Bakulin M. A. “Analysis and increasing the level of security of a significant object of critical information infrastructure” // Mavlyutov Readings: materials of the XV All-Russian Youth Scientific Conference: in 7 volumes, Ufa, October 26–28, 2021. Volume 4. Ufa: Ufa State Aviation Technical University, 2021. Pp. 331-342. (In Russian).]]

Поступила в редакцию 27 сентября 2023 г.

МЕТАДАННЫЕ / METADATA

Title: Risk management of information security violations of significant objects of critical information infrastructure.

Abstract: The article is devoted to the analysis and practical implementation of the stages of information security risk management of critical information infrastructure (CII). The process of pre-project analysis of the research object, identification of CII objects and their categorization, risk assessment using fuzzy cognitive maps and their reduction in accordance with the requirements of the regulatory framework that applies to significant CII objects is described. Reducing the risks of information security violations is implemented through the modernization of the information security system and the reorganization of the network. Possible options for risk treatment are being considered.

Key words: information security, critical information infrastructure, information security system, risks of information security violations, fuzzy cognitive maps, information security risk assessment, information security risk reduction.

Язык статьи / Language: русский / Russian.

Об авторе / About the author:

БАКУЛИН Михаил Алексеевич
ФГБОУ ВО «Уфимский университет науки и технологий», Россия.
Магистрант ин-та информатики, математики и робототехники. Иссл. в обл. информационной безопасности, защиты программного кода.
E-mail: bakulinmikhail@mail.ru

BAKULIN Mikhail Alekseyevich
Ufa University of Science and Technologies, Russia.
Master's student, Institute of Informatics, Mathematics, and Robotics. Research in the field of information security, software code protection.
E-mail: bakulinmikhail@mail.ru