Александр Н. Вавичкин[1], Виктор С. Горбатов[2], Анатолий П. Дураковский[3], Денис А. Чжен[4]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
[1]*e-mail: anvavichkin@mephi.ru, https://orcid.org/ 0000-0001-9755-2167*
[2]*e-mail: vsgorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733*
[3]*e-mail: apdurakovskiy@mephi.ru, http://orcid.org/0000-0002-8311-7735*
[4]*e-mail: world-denis16@mail.ru, https://orcid.org/0000-0002-2692-3837*

К ВОПРОСУ КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

DOI: http://dx.doi.org/10.26583/bit.2019.2.03

Аннотация. Целью статьи является упрощение деятельности по проведению категорирования объектов критической информационной инфраструктуры (КИИ) для образовательных организаций, осуществляющих научно-исследовательскую деятельность, в рамках выполнения принятого законодательства. В области обеспечения критической информационной безопасности до сих пор совершенствуется нормативно-законодательная база в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», возлагая на субъекты КИИ новые требования. Сфера образовательных услуг отсутствует в данной норме, соответственно, и автоматизированные информационные системы поддержки административных процессов управления, а также обеспечения образовательного процесса исключены из перечня объектов КИИ. Приведенный перечень содержит указание на сферу науки, и если какое-либо учреждение высшей школы указало в своем уставе научно-исследовательскую деятельность, оно становится субъектом данного законодательства, что накладывает на него обязанность проведения ряда организационно-технических мероприятий по обеспечению безопасности объектов КИИ. В статье приводится минимальный порядок действий при категорировании определенных перечнем объектов КИИ в сфере научной деятельности.

Ключевые слова: критическая информационная инфраструктура, методика категорирования, обеспечение безопасности значимого объекта.

Для цитирования: ВАВИЧКИН, Александр Н. et al. К ВОПРОСУ КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. Безопасность информационных технологий, [S.l.], v. 26, n. 2, p. 44-57, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1198>. Дата доступа: 30 may 2019. doi:http://dx.doi.org/10.26583/bit.2019.2.03.

Alexander N. Vavichkin[1], Viktor S. Gorbatov[2], Anatoly P. Durakovskiy[3], Denis A. Chzhen[4]
National Research Nuclear University MEPhI,
Kashirskoe sh., 31, Moscow, 115409, Russia
[1]*e-mail: anvavichkin@mephi.ru, https://orcid.org/ 0000-0001-9755-2167*
[2]*e-mail: vsgorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733*
[3]*e-mail: apdurakovskiy@mephi.ru, http://orcid.org/0000-0002-8311-7735*
[4]*e-mail: world-denis16@mail.ru, https://orcid.org/0000-0002-2692-3837*

To the issue of categorization of critical informational infrastructure objects in higher education

DOI: http://dx.doi.org/10.26583/bit.2019.2.03

Abstract. The aim of this work is to simplify the activities of categorization of critical information infrastructure (CII) for educational organizations engaged in research activities in the framework of the implementation of the adopted legislation. In the field of critical information security, the regulatory and legislative framework is still being improved in accordance with the Federal law "On the security of critical information infrastructure of the Russian Federation" dated 26.07.2017 No. 187-FZ, imposing

new requirements on the subjects of CII. The educational sphere is absent in this norm, as well as the automated information systems of support of administrative processes of management, and also ensuring educational process are excluded from the list of objects of CII respectively. However, the above list contains an indication of the sphere of science, and if any higher education institution is involved in research activities, it becomes the subject of this legislation, which imposes the obligation to carry out a number of organizational and technical measures to ensure the safety of CII facilities. The paper details the minimum procedures for categorization of a certain list of CII for the institutions involved in scientific research.

Keywords: critical information infrastructure, methods of categorization, ensuring the safety of a significant object

For citation: VAVICHKIN, Alexander N. et al. To the issue of categorization of critical informational infrastructure objects in higher education. IT Security (Russia), [S.l.], v. 26, n. 2, p. 44-57, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1198>. Date accessed: 30 may 2019. doi:http://dx.doi.org/10.26583/bit.2019.2.03.

Введение

В настоящее время наблюдается феномен широкой цифровизации всех сфер общественной деятельности с одной стороны и, как следствие, повышение уровня террористических и иных угроз, в том числе в условиях усиления международного противостояния в области обеспечения кибербезопасности, с другой стороны. Этим объясняется нынешнее особое внимание общественности и органов государственной власти к проблемам обеспечения информационной безопасности, поставленным в новой редакции соответствующей Доктрины[1].

Условно можно выделить два взаимосвязанных инфраструктурных направления государственной политики по практическому разрешению этих проблем. Первое – это развитие с учетом современных реалий, организационной инфраструктуры обеспечения, так называемой «офисной» кибербезопасности[2], где основным объектом защиты от компьютерных атак являются информационные ресурсы Российской Федерации. Вторым, относительно новым направлением, имеющим свои особенности, под условным наименованием «промышленная» кибербезопасность, является создание инфраструктуры безопасности так называемых киберфизических систем[3], обеспечивающих устойчивое управление и/или эксплуатацию потенциально опасных объектов в промышленности, транспорте, энергетике, связи и т.д. [1].

Первое направление деятельности в рассматриваемой области является относительно традиционным, уже имеющим обширную и относительно хорошо разработанную нормативно-правовую и методическую базу. Практическая реализация задач обеспечения «промышленной» кибербезопасности, в силу новизны законодательства по обеспечению безопасности объектов критической информационной инфраструктуры (КИИ), требует несколько иных подходов, необходимого толкования и разъяснения основных положений принятых нормативных актов, а также широкого обмена опытом различных субъектов КИИ, в частности, со стороны ведущих научно-образовательных центров нашей страны.

Такая работа активно проводится основным государственным уполномоченным регулятором в рассматриваемой области – ФСТЭК России в рамках различных

[1] Доктрина информационной безопасности Российской Федерации.

[2] 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»

[3] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

разъяснительных мероприятий, конференций [2], периодически проводятся вебинары на данную тематику [3]. На национальном форуме информационной безопасности «Инфофорум–2019», в частности, рассмотрены проблемы обеспечения безопасности критической информационной инфраструктуры оператора связи, вопросы реализации требований рассматриваемого законодательства в информационных системах транспортной отрасли и ряд других аспектов в части, касающейся защиты объектов КИИ [4]. На VI Федеральной конференции «Critical Communications Russia – Инновационные цифровые технологии для обеспечения безопасности государства, общества, бизнеса» даны практические советы, в частности, о том, что разработка, производство, ввод в эксплуатацию, эксплуатация в течение жизненного цикла и вывод из эксплуатации программных, программно-аппаратных комплексов, средств и систем должны выполняться в соответствии с требованиями к системам безопасности значимых объектов КИИ [5]. В работе [6] приведена традиционная схема жизненного цикла технической системы и сделан вывод применительно к рассматриваемым вопросам о том, что принятие неверных решений неминуемо отразится на проблемах эксплуатации системы.

Основная роль при оценке эффективности системы безопасности объектов КИИ отводится методам анализа эффективности затрат, которые позволяют установить связь между затратами и конечным результатом. Ведь кроме законодательных требований важным фактором практической реализации является достижение целей при минимальных затратах, в частности, за счет минимизации численности и/или снижения занятости персонала.

В работе [7] применительно к киберфизическим системам, функционирующим в процессах управления сложными, потенциально опасными объектами, выделены следующие факторы обеспечения их безопасности: адекватность, оптимальность, оперативность, устойчивость, непрерывность, скрытность. При этом состояние защищенности определяется на основе оценки их киберустойчивости.

Тем не менее процесс практической реализации конкретных задач по обеспечению «промышленной» кибербезопасности находится пока еще на начальной стадии, поэтому актуальным вопросом является обсуждение указанных проблем применительно к конкретным организационным структурам, в частности, к учреждениям высшей школы, что и является предметом настоящей статьи. Несмотря на то, что факт невыполнения основных требований законодательства вузами не предусматривает какой-либо ответственности (см. [8]), по факту того или иного инцидента или компьютерной атаки с нанесением существенного ущерба может наступить юридическая ответственность в соответствии с расширенной статьей 274.1 Уголовного кодекса Российской Федерации[4].

В настоящей работе приводится обоснование отнесения вузов к субъектам законодательства о безопасности объектов критической информационной инфраструктуры, рассмотрен вопрос выделения соответствующих объектов и создания их перечней, особенности категорирования таких объектов по установленным критериям безопасности, даются некоторые рекомендации по реализации требований и созданию систем обеспечения безопасности объекта КИИ.

1. Вуз как субъект законодательства о безопасности КИИ

Субъектность того или иного законодательства устанавливается соответствующей нормой базового (основного) закона, каким для рассматриваемой предметной области является Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической

[4]Уголовный кодекс Российской Федерации

информационной инфраструктуры Российской Федерации». В соответствии со статьей 2 (пункт 8) субъектом критической информационной инфраструктуры признается структура, которой «…на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, 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) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей». Как видно, в данной норме отсутствует указание на сферу образовательных услуг, из чего следует вывод о том, что автоматизированные информационные системы поддержки административных процессов управления, а также обеспечения образовательного процесса исключены из перечня объектов КИИ.

Тем не менее приведенный перечень содержит указание на сферу науки. Поэтому в соответствии с разъяснением уполномоченного государственного регулятора в области безопасности объектов КИИ – ФСТЭК России [2], если какое-либо учреждение высшей школы указало в своем уставе научно-исследовательскую деятельность, оно по крайней мере формально становится субъектом данного законодательства, что накладывает на него обязанность проведения ряда организационных мероприятий:

Их суть:

1. Инвентаризацию автоматизированных информационных систем управления, используемых при проведении НИОКР с целью отнесения (или исключения) их к объектам критической инфраструктуры по критерию потенциальной возможности нанесения существенного ущерба в случае нештатной ситуации (режима работы).

2. Экспертизу итогов инвентаризации на уровне специально созданной комиссии и утверждение на уровне руководства вуза соответствующего перечня объектов КИИ, направляемого на согласование уполномоченному государственному регулятору.

3. Категорирование выделенных объектов КИИ с целью установления их соответствия нормативно установленным значениям показателей критериев значимости и присвоение каждому из них одной из соответствующей категории либо принятие решения об отсутствии необходимости присвоения такой категории значимости[5].

Содержательным итогом такой работы является решение о необходимости (или об отсутствии необходимости) проведения работ по созданию необходимой системы безопасности объекта, сводящей риски возникновения нештатных ситуаций до приемлемых величин. Так как указанные выше организационные мероприятия являются относительно новыми для научно-исследовательских подразделений вузов, рассмотрим более подробно процесс категорирования объектов КИИ применительно к учреждению высшей школы.

2. Категорирование объектов КИИ вуза

Из общего анализа законодательных требований по безопасности КИИ применительно к вузам следует, что к таким объектам прежде всего относятся сложные экспериментальные установки, использующие автоматизированные подсистемы управления, особенно интегрированные в территориально разнесенные сетевые структуры. Учитывая то, что такими объектами обладают только ведущие вузы

[5]Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127.

технического профиля, такое выделение не является сложной организационной задачей, выполнение которой не требует значительных ресурсов. Основной же объем затрачиваемых в процессе категорирования ресурсов приходится на проведение относительно новых для экспериментаторов и/или органов управления следующих работ:

– создание «модели нарушителя» [9], то есть рассмотрение возможных типов нарушителей и/или их действий в отношении данного объекта;

– анализ уязвимостей и соответствующих угроз безопасности управляющей информации, которые могут привести к возникновению компьютерных инцидентов, связанных с нештатным режимом функционирования объекта КИИ;

– оценка в соответствии с установленным перечнем показателей критериев значимости[6] масштаба возможных последствий в случае возникновения компьютерных инцидентов и установление объекту КИИ одной из категорий значимости либо принятие решения об отсутствии такой необходимости.

Основой процесса категорирования объектов КИИ является анализ уязвимостей и актуальных угроз, который можно осуществить, как правило, путем использования соответствующей базы данных ФСТЭК России [10, 11] и возможностей актуальных нарушителей в отношении объектов критической информационной инфраструктуры.

Необходимость проведения анализа этого основного этапа определяется специальной комиссией учреждения высшей школы по категорированию, а исходными данными являются сведения о программно-аппаратных средствах, общесистемном программном обеспечении, прикладном программном обеспечении и средствах защиты информации, используемых на рассматриваемой экспериментальной установке.

Соответствующий алгоритм действий по созданию перечней потенциальных уязвимостей приведен на рис. 1.

Рекомендованный порядок действий при формировании перечня потенциальных уязвимостей:

– с помощью браузера открыть web-страницу http://www.bdu.fstec.ru/vul, базы данных уязвимостей ФСТЭК России;

– осуществить выгрузку уязвимостей в формат *.excel с помощью гиперссылки на web-странице «Скачать сведения об уязвимостях в формате XLSX» и переименовать файл vullist.xlsxв «Уязвимости <Наименование объекта критической информационной инфраструктуры>.xlsx»;

– с помощью системы фильтров отобразить перечень для конкретных типов программно-аппаратных средств, программного обеспечения и средств защиты информации, применяемых на объекте критической информационной инфраструктуры, в следующем порядке:

а) «Вендор ПО» - выбрать производителей, применяемых на объекте критической информационной инфраструктуры;

б) «Тип ПО» - выбрать типы программного обеспечения, применяемого на объекте критической информационной инфраструктуры;

в) «Название ПО» - выбрать наименования программного обеспечения, применяемого на объекте критической информационной инфраструктуры;

г) «Версия ПО» - выбрать версию программного обеспечения, применяемого на объекте критической информационной инфраструктуры. При указании версии

[6]Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения, утвержденный постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

необходимо учитывать, что версия программного обеспечения может встречаться в нескольких строках фильтра;

– перечень потенциальных уязвимостей сохранить в электронном виде.

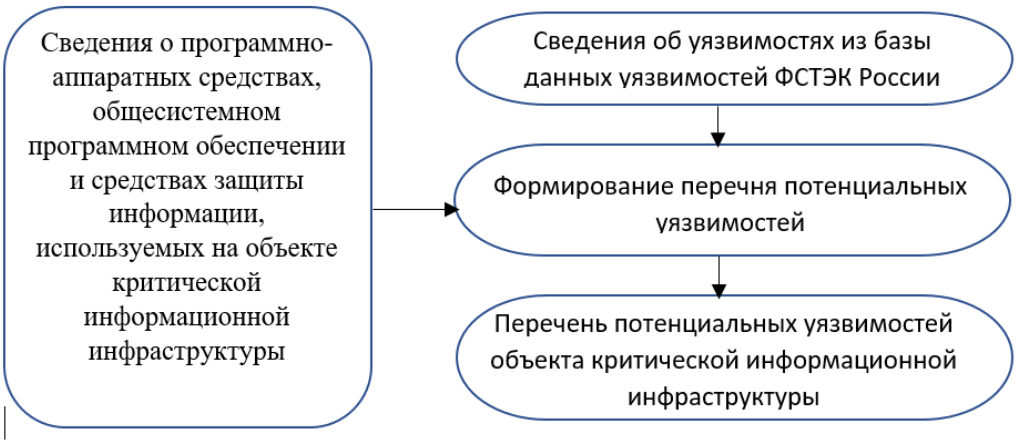

Рис. 1. Процедура формирования перечня потенциальных уязвимостей
(Fig. 1. Procedure for creating a list of potential vulnerabilities)

На рис. 2 показан алгоритм действий по анализу угроз безопасности управляющей информации на объекте КИИ, на основании которого утверждается список актуальных угроз с последующей оценкой возможных масштабов ущерба от нештатного режима вследствие компьютерного инцидента.

Рекомендуемый порядок анализа УБИ:

1. С помощью браузера открыть web-страницу http://www.bdu.fstec.ru/threat, базы данных УБИ ФСТЭК России.

2. Осуществить выгрузку УБИ в формат *.excel с помощью гиперссылки на web-странице «Скачать сведения об угрозах». Переименовать файл thrlist.xlsxв «Угрозы <Наименование объекта критической информационной инфраструктуры>.xlsx».

3. С помощью системы фильтров отобразить перечень угроз безопасности информации, применимых для объекта критической информационной инфраструктуры, с учетом потенциала актуальных нарушителей для данного объекта критической информационной инфраструктуры:

– объект воздействия устанавливается путем фильтрации объектов воздействия в зависимости от используемых компонентов объекта критической информационной инфраструктуры;

– источник угроз устанавливается согласно ранее полученным результатам. При установке потенциала источника угроз необходимо учитывать, что нарушитель с потенциалом более высокого уровня имеет возможность реализовать угрозы нарушителя с потенциалом более низкого уровня.

4. Добавить в файл столбцы «Анализ угрозы», «Актуальность угрозы» и «Тип инцидента».

5. Выполнить анализ каждой УБИ, применимой к объекту критической информационной инфраструктуры. Результаты анализа УБИ оформляются в рабочих материалах по категорированию объекта критической информационной инфраструктуры.

Рекомендуется выполнить анализ влияния уязвимостей на возникновение УБИ. Необходимость выполнения следующих действий определяется комиссией по категорированию.

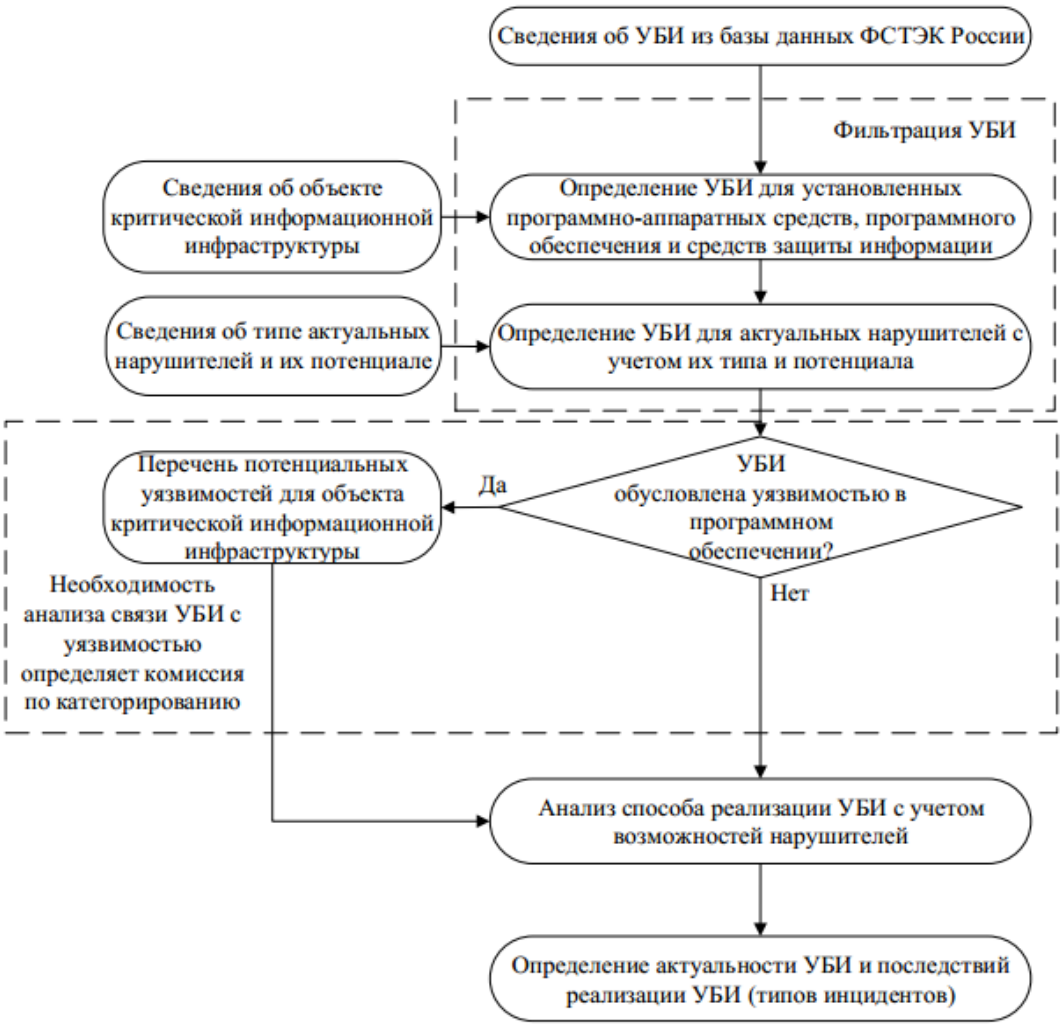

Рис. 2. Процедура анализа угроз беопасности
(Fig. 2. Safety hazard analysis procedure)

Если УБИ обусловлена уязвимостью в программном обеспечении, то осуществить поиск уязвимостей в файле «Уязвимости <Наименование объекта критической информационной инфраструктуры>.xlsx» (полученном по результатам выполнения предыдущих действий), посредством которых возможно реализовать УБИ из перечня потенциальных уязвимостей.

При анализе уязвимостей необходимо принимать во внимание класс уязвимостей, а именно:

– уязвимости класса «уязвимость кода» всегда актуальны вне зависимости, выполнены ли мероприятия по их устранению или нет;

– уязвимости класса «уязвимость архитектуры» требуют анализа архитектуры объекта для определения ее актуальности. Пример неактуальной уязвимости, если в архитектуре объекта отсутствуют беспроводная сеть, использующая протокол WPA2 (идентификатор BDU:2017-02269): «Уязвимость протокола WPA2, связанная с ошибками управления криптографическими ключами (STK-key) и позволяющая получить доступ к зашифрованной информации, передаваемой по беспроводной сети».

Определить способ реализации УБИ (учитываются возможности нарушителей и архитектура объекта). При определении способа реализации УБИ необходимо учитывать

то, что УБИ могут быть реализованы непосредственно за счет доступа к компонентам системы и (или) информации или опосредовано (косвенно) за счет создания условий и (или) средств, обеспечивающих такой доступ. Оценка масштаба последствий проводится на основе анализа возможных сценариев нарушения штатного режима функционирования объекта КИИ (функций автоматизации) и соответствующего ущерба в случае их реализации. В зависимости от величины ущерба, устанавливаемой экспертным путем, определяются показатели значимости, установленные в соответствующих правилах категорирования[7]. Анализ соответствия установленных показателей значимости объектов КИИ проведен применительно к научно-исследовательской деятельности технического вуза. В табл.1 указаны только применимые показатели критериев значимости объектов КИИ для вузов.

Таблица 1. Применимые показатели критериев значимости объектов КИИ вуза

Критерий значимости	**Показатель**	**Применимость для вуза**
Социальная значимость	Причинение ущерба жизни и здоровью людей	(+) При нештатных ситуациях эксплуатации экспериментальных установок возможно причинение ущерба, по крайней мере, здоровью персонала
Экономическая значимость	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности	(+) При невыполнении или срыве сроков выполнения научно-исследовательских проектов возможно снижение уровня дохода по основным видам деятельности вуза
Экологическая значимость	Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия)	(+) При нештатных ситуациях эксплуатации экспериментальных установок возможен выброс вредных веществ в окружающую среду
Значимость для обеспечения обороны страны, безопасности государства и правопорядка	Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры	(+) В случае взаимодействия с государственными органами в части исполнения оборонных заказов
	Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю	(+)

[7]Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

Таким образом, из анализа данных таблицы 1 следует, что лишь незначительная часть установленных показателей значимости применима для научных подразделений учреждений высшей школы.

В соответствии с пунктом 7 рассматриваемых правил категорирования объектов КИИ[8] устанавливаются три категории значимости, из которых самая высокая категория - первая, соответствующая наиболее крупному потенциальному ущербу. Численные значения, соответствующие границам указанных категорий, приведены в правилах категорирования[8].

В случае если объект КИИ (автоматизированная подсистема управления экспериментальной установки) не соответствует ни одной из категорий, процедуры выполнения нормативных требований законодательства в области безопасности объектов КИИ заканчиваются при условии оформления соответствующих актов.

3. Практический пример категорирования

Продемонстрируем указанные выше процедуры на примере категорирования объекта КИИ, в качестве которого выберем блок управления часто используемых в научных экспериментах рентгенотелевизионной установки неразрушающего контроля предметов исследования. Все сведения по штатной (безопасной) эксплуатации такой установки содержатся в руководстве по эксплуатации и инструкции пользователя.

Выбор указанного объекта предопределяет указание в Руководстве по эксплуатации в разделе «Радиационная безопасность» на то, что рентгеновская трубка является техногенным источником ионизирующего (рентгеновского) излучения, представляющего потенциальную опасность для здоровья персонала.

Все компоненты установки взаимодействуют между собой с помощью специализированного программного обеспечения, установленного на блоке управления, при этом возможность воздействия (потенциальные уязвимости и угрозы безопасности управляющей информации) имеется лишь при наличия доступа к блоку управления. Таким образом, исходными данными для категорирования рассматриваемого объекта являются сведения о прикладном и общесистемном ПО для блока управления. Как правило, в качестве общесистемного ПО используется та или иная версия Microsoft Windows. Тип предустановленного прикладного ПО зависит от марки конкретной рентгенотелевизионной установки. Иное прикладное ПО не предусмотрено, а специализированные средства защиты информации не применяются. Следует отметить, что блок управления имеет возможность подключения устройств с помощью интерфейса USB.

Разработка модели нарушителя проводится на основе экспертной оценки типов нарушителей [12], их потенциала и мотивации по совершению противоправной деятельности (табл. 2).

Актуальность нарушителя определяется в соответствии с табл. 3.

Для версии системного ПО Microsoft Windows управляющего системой либо распространяющиеся на всю линейку операционных систем Windows (табл. 4).

Потенциальные угрозы безопасности управляющей информации, а также их актуальность по отношению к рентгенотелевизионной установке определяются

[8]Правила категорирования объектов критической информационной инфраструктуры Российской Федерации утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127

экспертным методом либо по любой из методик определения актуальных угроз, выпущенных ФСТЭК России [13].

Таблица 2. Используемые экспертные значения для определения актуальности нарушителей

Нарушитель	**Уровень мотивации нарушителя**	**Потенциал нарушителя**	**Актуальность нарушителя**
Внешний нарушитель			
Криминальные структуры	Низкий	Средний	Неактуален
Недобросовестные партнеры	Низкий	Средний	Неактуален
Иные юридические лица	Низкий	Средний	Неактуален
Высококвалифицированные взломщики компьютерных систем	Низкий	Высокий	Актуален
Бывшие сотрудники организации	Высокий	Средний	Актуален
Поставщики программного обеспечения и технических средств	Минимальный	Средний	Неактуален
Разработчики программного обеспечения	Низкий	Средний	Неактуален
Внутренний нарушитель			
Лица, являющиеся зарегистрированными пользователями системы	Средний	Средний	Актуален
Лица, являющиеся зарегистрированными пользователями системы с полномочиями системного администратора	Средний	Высокий	Актуален
Лица, являющиеся зарегистрированными пользователями системы с полномочиями администратора информационной безопасности	Средний	Средний	Актуален

Таблица 3. Матрица определения актуальности нарушителя

Уровень мотивации нарушителя	**Потенциал нарушителя**		
	Низкий	**Средний**	**Высокий**
Минимальный	Неактуален	Неактуален	Неактуален
Низкий	Неактуален	Неактуален	Актуален
Средний	Неактуален	Актуален	Актуален
Высокий	Актуален	Актуален	Актуален
Крайне высокий	Актуален	Актуален	Актуален

Таблица 4. Потенциальные уязвимости ПО Microsoft Windows

Идентификатор	**Наименование уязвимости**	**Описание уязвимости**	**Уровень опасности уязвимости**
BDU:2017-00008	Уязвимость операционной системы Windows, позволяющая нарушителю обойти проверку сертификата	Уязвимость скрипта PowerShell ОС Windows из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему локально, обойти проверку сертификата	Низкий уровень опасности (базовая оценка CVSS 2.0 составляет 2,1)
BDU:2019-00540	Уязвимость RDP-клиента операционной системы Windows, позволяющая нарушителю выполнить произвольный код	Уязвимость RDP-клиента (mstsc .exe) операционной системы Windows связана с недостатками механизмов безопасности при использовании в процессе удаленного соединения общего буфера обмена. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код путем компрометации или подмены RDP-сервера	Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10) Высокий уровень опасности (базовая оценка CVSS 3.0 составляет 8,8)

Угрозы фиксируются в форме, указанной в табл.5.

Таблица 5. Угрозы безопасности информации для рентгенотелевизионной установки

Идентификатор УБИ	Наименование УБИ	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объекты воздействия	Анализ угрозы (используемая уязвимость, способ реализации угрозы)	Актуальность угрозы	Последствия реализации УБИ/ тип инцидента
22	Угроза избыточного выделения оперативной памяти	Угроза заключается в возможности выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти, доступных в системе для выделения в ответ на запросы программ легальных пользователей. Угроза обусловлена наличием слабостей механизма контроля выде ления оперативной памяти различным программам. Реализация угрозы возможна при условии нахождения вредоносного программного обеспечения в системе в активном состоянии	Внешний нарушитель с низким потенциалом. Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, сетевое программное обеспечение	Возможность реализации угрозы обуслов лена наличием возможности подключения внешних носителей, а также ошибками в ПО	Актуальна	Отказ в обслуживании
…	…	…	…	…	…	…	…

Реализация УБИ для рентгенотелевизионной установки может привести к возникновению следующих компьютерных инцидентов, указанных в табл. 6.

Таблица 6. Компьютерные инциденты на объекте КИИ рентгенотелевизионной установки

Тип компьютерного инцидента	Описание компьютерного инцидента
Отказ в обслуживании	- Прекращение функционирования установки из-за неработоспособного прикладного и общесистемного ПО Блока управления; - нарушение доступности управляющей информации
Утечка данных (нарушение конфиденциальности)	- Раскрытие управляющей информации неограниченному кругу лиц может быть использована для развития компьютерной атаки
Несанкционированный доступ	- Несанкционированное управление, приводящее к нештатной ситуации; - нарушение установленных правил разграничения доступа к техническим средствам рентгенотелевизионной установки (получение физического доступа)
Модификация (подмена) данных	- Изменение общесистемного и прикладного ПО, приводящее к замедлению либо прерыванию их функционирования; - нарушение целостности управляющей информации
Нарушение функционирования технических средств	- Нарушение функционирования компонентов рентгенотелевизионной установки; - скрытное изменение параметров установок в пределах допустимых значений
Несанкционированное использование вычислительных ресурсов объекта	Нарушение функционирования рентгенотелевизионной установки вследствие воздействия на ПО (снижение производительности компонентов системы)

В соответствии с данными табл. 1 укажем на применимость установленных показателей критериев значимости для рентгенотелевизионной установки (табл. 7).

Таблица 7. Показатели критериев значимости для рентгенотелевизионной установки

Показатель значимости	**Значение показателя**
Причинение ущерба жизни и здоровью людей	Количество возможных санитарных потерь (КЛ): до 50 человек. Категория - III
Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности	Д = 0. Расходы, понесенные от кратковременного простоя, не приведут к снижению планового уровня доходов за квартал. Категория - не присваивается
Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры	Показатель неприменим. Объект не используется для выполнения государственного оборонного заказа. Категория - не присваивается

Присвоение рентгенотелевизионной установке III категории значимости осуществляется исходя из установленного показателя возможного причинения ущерба жизни и здоровью людей в количестве до 50 человек. Такой ущерб при возникновении нештатной ситуации можно объяснить либо некомпетентной эксплуатацией, либо возникновением компьютерных инцидентов. Очевидно, что исключается возможность нанесения ущерба жизни и здоровью людей при отсутствии взаимодействия между всеми узлами установки, то есть в нерабочем состоянии.

Также признается крайне маловероятной возможность использования установки с целью предумышленного нанесения ущерба жизни и здоровью людей. Расчёт количество людей, жизни и здоровью которых возможно причинение ущерба, рассчитывается по формуле [13]:

$$N = N_{без} + N_{сан},$$

где: N – количество людей, которым возможно причинение ущерба;

Nбез – количество безвозвратных потерь, чел.;

Nсан – количество санитарных потерь, чел.

Таким образом, для рентгенотелевизионной установки присваивается III категория значимости. После присвоения категории значимости оформляется акт категорирования в произвольной форме, а также формируются сведения для передачи во ФСТЭК России в соответствии с утвержденной ФСТЭК России формой[9]. Далее на основе проведенного категорирования производится выработка защитных мер, призванных минимизировать риски возникновения компьютерных инцидентов, а также сократить ущерб в случае их возникновения

[9] 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".

Заключение

Таким образом, из анализа рекомендаций уполномоченного государственного регулятора в области обеспечения безопасности объектов КИИ следует, что учреждения высшей школы в той или иной степени могут быть отнесены к субъектам соответствующего законодательства, причем на данном этапе выполнение нормативных положений не является сложной организационно-технической задачей, требующей значительных затрат. Тем не менее развитие киберфизических систем, в частности интернета вещей, и их внедрение в практическую деятельность учреждений высшей школы может привести к пересмотру такого положения, что указывает на необходимость обязательного учета рассмотренных выше положений в ходе автоматизации различных бизнес-процессов и прежде всего при расширении материально-технической базы экспериментальных исследований.

СПИСОК ЛИТЕРАТУРЫ:

1. Касперский, Е.В. В заложниках у автоматики: как защитить промышленность от кибератак. Безопасность информационных технологий, [S.l.]. Том 23, №3. С. 7−10, oct. 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/12 (дата обращения: 06.04.2019).
2. Лютиков В.С. О безопасности критической информационной инфраструктуры Российской Федерации. Шестая конференция «Информационная безопасность автоматизированных систем управления технологическими процессами критически важных объектов». 27−28 февраля 2018 г. МТУСИ. URL: http://www.ибкво.рф/wp-content/uploads/2018/11/001_116_Connect_03_2018_Sm-24-36.pdf (дата обращения: 23.01.2019).
3. Литвиненко В.А. О мерах по реализация Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». 27 сентября 2018 г. МИРЭА-РТУ. URL: https://www.youtube.com/watch?v=X0iWKjbdAHM (дата обращения: 23.01.2019).
4. Программа конференций: Национальный форум информационной безопасности «Инфофорум» - Москва, 2018. URL: https://infoforum.ru/conference/conference/program/cid/42 (дата обращения: 23.01.2019).
5. Масановец В.В. Как правильно обеспечить безопасность объектов критической информационной инфраструктуры. Советы практикам: 6-я Федеральная конференция «Critical Communications Russia– Инновационные цифровые технологии для обеспечения безопасности государства, общества, бизнеса» Масановец В.В. – Москва, 2017. URL: https://ru-bezh.ru/kak-pravilno-obespechit-bezopasnost-obektov-kriticheskoj-informa (дата обращения: 23.01.2019).
6. Чобанян В.А. [электронный ресурс]: Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры. - / Чобанян В.А., Шахалов И.Ю. – Электрон. дан. – 2013. URL: https://cyberleninka.ru/article/v/analiz-i-sintez-trebovaniy-k-sistemam-bezopasnosti-obektov-kriticheskoy-informatsionnoy-infrastruktury (дата обращения: 23.01.2019).
7. Захарченко Р.И. [электронный ресурс]: Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве. - / Захарченко Р.И., Королев И.Д. – Электрон. дан. – 2018. URL: https://cyberleninka.ru/article/n/metodika-otsenki-ustoychivosti-funktsionirovaniya-obektov-kriticheskoy-informatsionnoy-infrastruktury-funktsioniruyuschey-v (дата обращения: 23.01.2019).
8. Гродзенский Яков. [электронный ресурс]: Как защитить КИИ в соответствии с 187-ФЗ - Гродзенский Яков. - Электрон. дан. URL: https://www.anti-malware.ru/practice/solutions/critical-infrastructure-security-187 (дата обращения 23.01.2019).
9. Чернов Денис Владимирович, Сычугов Алексей Алексеевич ФОРМАЛИЗАЦИЯ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП. Известия ТулГУ. Технические науки. 2018. №10. URL: https://cyberleninka.ru/article/n/formalizatsiya-modeli-narushitelya-informatsionnoy-bezopasnosti-asu-tp (дата обращения: 28.04.2019).
10. База данных уязвимостей [электронный ресурс]. PositiveTechnologies. – Электрон. дан. URL: https://www.securitylab.ru/vulnerability (дата обращения 18.01.2019).
11. Банк данных угроз безопасности информации ФСТЭК России [электронный ресурс]. ФСТЭК России. – Электр. дан. URL: http://www.bdu.fstec.ru/vul (дата обращения 18.01.2019).

12. Методика определения угроз информационной безопасности в информационных системах URL: https://fstec.ru/component/attachments/download/812 (дата обращения 18.01.2019).
13. Единая межведомственная методика оценки ущерба от чрезвычайных ситуаций техногенного, природного и террористического характера, а также классификации и учета чрезвычайных ситуаций – М.: ФГУ ВНИИ ГОЧС (ФЦ), 2004 г.

REFERENCES:

[1] Kaspersky, E. V. Automation hostage: how to protect the industry againts cyber attacks. IT Security (Russia), [S.l.]. V. 23, n. 3. P. 7−10, oct. 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/12 (accessed: 06.05.2019). (in Russian).
[2] Lyutikov V.S. On security of critical information infrastructure of the Russian Federation. 6th conference "Information security of automated process control systems of critical facilities". February 27-28, 2018. MTUCI. URL: http://www.ибквo.рф/wp-content/uploads/2018/11/001_116_Connect_03_2018_Sm-24-36.pdf (accessed: 23.01.2019). (in Russian).
[3] Litvinenko V. A. On measures to implement the Federal law of July 26, 2017 № 187-FZ "On security of critical information infrastructure of the Russian Federation". 27 September 2018 MIREA-RTU. URL: https://www.youtube.com/watch?v=X0iWKjbdAHM (accessed: 23.01.2019). (in Russian).
[4] Conference program: national forum of information security "Infoforum" - Moscow, 2018. URL: https://infoforum.ru/conference/conference/program/cid/42 (accessed: 23.01.2019). (in Russian).
[5] Masanovets V. V. How to ensure the security of critical information infrastructure. Tips for practice: 6th Federal conference "Critical Communications Russia — Innovative digital technologies to ensure the security of the state, society, business". - Moscow, 2017. URL: https://ru-bezh.ru/kak-pravilno-obespechit-bezopasnost-obektov-kriticheskoj-informa (accessed: 23.01.2019). (in Russian).
[6] Chobanyan V. A., Shakhalov I. Yu. Analysis and synthesis of requirements to security systems of critical information infrastructure.– 2013. URL: https://cyberleninka.ru/article/v/analiz-i-sintez-trebovaniy-k-sistemam-bezopasnosti-obektov-kriticheskoy-informatsionnoy-infrastruktury (accessed: 23.01.2019). (in Russian).
[7] Zakharchenko R. I., Korolev I. D. Methods of assessing the stability of the critical information infrastructure functioning in cyberspace. 2018. URL: https://cyberleninka.ru/article/n/metodika-otsenki-ustoychivosti-funktsionirovaniya-obektov-kriticheskoy-informatsionnoy-infrastruktury-funktsioniruyuschey-v (accessed: 23.01.2019). (in Russian).
[8] Grodzenskiy Yakov. How to protect CUES in accordance with 187-FZ. URL: https://www.anti-malware.ru/practice/solutions/critical-infrastructure-security-187 (accessed: 23.01.2019). (in Russian).
[9] Chernov Denis V., Sychugov Alexei A. The formalization of an intruder model of information security of APCS. Izvestia TulGU. Technical science.2018. №10. URL: https://cyberleninka.ru/article/n/formalizatsiya-modeli-narushitelya-informatsionnoy-bezopasnosti-asu-tp (accessed: 28.04.2019). (in Russian).
[10] Vulnerability database. PositiveTechnologies. URL: https://www.securitylab.ru/vulnerability (accessed: 18.01.2019). (in Russian).
[11] Data Bank of threats to information security of FSTEC of Russia. URL: http://www.bdu.fstec.ru/vul (accessed: 18.01.2019). (in Russian).
[12] Methods of determining threats to information security in information systems. URL: https://fstec.ru/component/attachments/download/812 (accessed: 18.01.2019). (in Russian).
[13] The interagency method of assessment of damages from emergency situations of technogenic, natural and terrorist nature, as well as the classification and accounting for emergencies – M.: FGU VNII GOCHS (FC), 2004. (in Russian).

Поступила в редакцию – 25 февраля 2019 г. Окончательный вариант – 25 мая 2019 г.
Received – February 25, 2019. The final version – May 25, 2019.