Министерство образования Республики Беларусь
Белорусский государственный университет
Юридический факультет
Кафедра конституционного права

СОГЛАСОВАНО
Заведующий кафедрой
_____Василевич Г.А.
«15» сентября 2023 г.

СОГЛАСОВАНО
Декан факультета
_____Шидловский А.В.
«30» ноября 2023 г.

Организационно-правовое обеспечение информационной безопасности

Электронный учебно-методический комплекс для специальности:
7-06-0421-01 «Юриспруденция»

Регистрационный № 2.4.2-24/431

Составитель:
Абламейко М.С. доцент кафедры конституционного права юридического факультета БГУ, кандидат юридических наук, доцент.

Рассмотрено и утверждено на заседании Научно-методического совета БГУ 29.02.2024 г., протокол № 5.

Минск 2023

УДК 34:002(075.8)
О-641

Утверждено на заседании Научно-методического совета БГУ
Протокол № 5 от 29.02.2024 г.

Решение о депонировании вынес:
Совет юридического факультета
Протокол № 3 от 30.11.2023 г.

Составитель:
Абламейко Мария Сергеевна, доцент кафедры конституционного права юридического факультета БГУ, кандидат юридических наук, доцент.

Рецензенты:
Михалева Т.Н., ведущий научный сотрудник Национального центра законодательства и правовых исследований Республики Беларусь, кандидат юридических наук, доцент;
Михайловский В.С., зав. кафедрой государственного управления юридического факультета БГУ, кандидат политических наук, доцент.

Организационно-правовое обеспечение информационной безопасности : электронный учебно-методический комплекс для специальности: 7-06-0421-01 «Юриспруденция» / БГУ, Юридический фак., Каф. конституционного права ; сост. М. С. Абламейко. – Минск : БГУ, 2023. – 59 с. – Библиогр.: с. 51–59.

Электронный учебно-методический комплекс (ЭУМК) по учебной дисциплине «Организационно-правовое обеспечение информационной безопасности» предназначен для магистрантов специальности 7-06-0421-01 «Юриспруденция». ЭУМК включает конспект лекций по вопросам учебной дисциплины, планы семинарских занятий, темы рефератов, а также список литературы.

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Электронный учебно-методический комплекс (ЭУМК) «Организационно-правовое обеспечение информационной безопасности» разработан для магистрантов специальности 7-06-0421-01 «Юриспруденция».

Комплекс подготовлен в соответствии с требованиями Положения об учебно-методическом комплексе на уровне высшего образования, утвержденного Постановлением Министерства образования Республики Беларусь от 26.07.2011 № 167.

Содержание разделов ЭУМК соответствует образовательным стандартам данной специальности, структуре и тематике учебной программы по дисциплине «Организационно-правовое обеспечение информационной безопасности».

Учебная дисциплина «Организационно-правовое обеспечение информационной безопасности» представляет собой совокупность научных знаний о подходах в сфере обеспечения информационной безопасности как составной части национальной безопасности, последних тенденциях развития информационного общества и электронного государства, особенностях международного опыта при противодействии угрозам информационной безопасности.

Цель и задачи учебной дисциплины

Цель учебной дисциплины «Организационно-правовое обеспечение информационной безопасности» – расширение и углубление знаний магистрантов по вопросам обеспечения информационной безопасности, полученным ранее в процессе изучения курса информационного права, конституционного права и других юридических дисциплин, приведения их в единую систему, способствующую более целостной и качественной профессиональной подготовке юриста.

Задачи учебной дисциплины:

1. Углубленно и комплексно рассмотреть понятие информационной безопасности, как составной части национальной безопасности Республики Беларусь, международно-правовой опыт в сфере информационной безопасности, внешние и внутренние угрозы, отдельные категории информации ограниченного доступа непосредственно связанные с обеспечением информационной безопасности; выявить пробелы и несоответствия в законодательстве, сложности его применения и пути их преодоления; изучить закономерности и проследить динамику развития информационной безопасности на современном этапе становления Республики Беларусь;
2. Сформировать умения выявления проблемных сфер в сфере информационной безопасности и навыки нахождения путей разрешения;
3. Сформировать у магистрантов навыки владения методов обеспечения информационной безопасности;
4. Обеспечить надлежащее усвоение студентами теории и практики применения систем защиты информации;

5. Повысить уровень общей правовой культуры магистрантов и создать условия для успешной профессиональной деятельности магистрантов благодаря глубоким знаниям и умениям применять эти знания на практике;

В результате изучения курса «Организационно-правовое обеспечение информационной безопасности» у магистратов должно сформироваться целостное представление о последних тенденциях развития обеспечения информационной безопасности и др.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием (магистра).

Учебная дисциплина относится к модулю «Цифровизация права и управления» компонента учреждения высшего образования.

В результате освоения учебной дисциплины студент должен:

знать:

сущность и систему обеспечения информационной безопасности; международные подходы в сфере обеспечения информационной безопасности, понятие внутренних и внешних угроз информационной безопасности, отдельные категории информации ограниченного доступа непосредственно связанные с обеспечением информационной безопасности.

уметь:

- анализировать источники в сфере обеспечения информационной безопасности, грамотно излагать свои суждения по вопросу информационной безопасности, систематизировать правовые требования к осуществлению и государственному регулированию обеспечения информационной безопасности, как составной части национальной безопасности Республики Беларусь, формулировать и обосновывать свою точку зрения по спорным вопросам.

владеть:

- понятийным аппаратом информационной безопасности, навыками анализа законодательства в сфере защиты информации и практики его применения в Республике Беларусь, навыками анализа законодательства зарубежных государств в сфере информатизации, навыками поиска необходимой информации для пополнения профессиональных знаний.

Теоретический раздел включает конспект лекций. Данный раздел содержит логично структурированный теоретический материал по всем вопросам дисциплины, который может быть использован для самостоятельной подготовки студентов к лекциям и семинарским занятиям.

Практический раздел содержит примерные планы семинарских занятий и темы рефератов.

Раздел контроля знаний включает примерный перечень вопросов к зачету.

Вспомогательный раздел содержит список рекомендуемой литературы (основной, нормативной и дополнительной) и ссылки на образовательные ресурсы.

1. ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

1.1. Основные понятия и определения в области информационной безопасности

Теория информационной безопасности. Этапы развития. Предметная область информационной безопасности.

Подходы к определению информационной безопасности. Термины, определяющие научную основу информационной безопасности. Термины, определяющие предметную основу информационной безопасности. Термины, определяющие характер деятельности по обеспечению информационной безопасности.

Составляющие информационной безопасности: доступность, конфиденциальность, целостность, достоверность информации.

Проблемы информационной безопасности общества.

Теория информационной безопасности наука сравнительно молодая. Свое развитие она получила в связи с бурным развитием информационных технологий, радиоэлектроники и связи и необходимостью сохранения информационных ресурсов. Как и любая другая наука, информационная безопасность имеет свой понятийный аппарат, который способен наиболее точно охарактеризовать все аспекты защиты информации. Многие понятия по своему содержанию соответствуют зарубежным аналогам. В то же время некоторые термины не являются устоявшимися и не всегда точно и полно характеризуют какой- либо процесс, свойство или предмет.

Отметим, что термин «компьютерная безопасность» (как эквивалент понятия «информационная безопасность») представляется слишком узким. Компьютеры – только одна из составляющих информационных систем, и хотя в первую очередь внимание будет сосредоточено на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на листочке, прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, средства коммуникаций и, конечно, обслуживающий персонал. Эта инфраструктура имеет самостоятельную ценность.

Множество понятий и терминов информационной безопасности отражает широкий спектр отличительных существенных свойств, признаков и отношений, присущих данному специфическому виду безопасности. Многие авторы (О. В. Азамов, К. Ю. Будылин, Е. Г. Бунев, С. А. Сакун, Д. Н. Шакин) выделяют три группы терминов теории информационной безопасности.

Термины, определяющие научную основу информационной безопасности

По мнению авторов к этой группе относятся термины, которые используются во многих областях знаний и являются однозначными, семантически унифицированными и стилистически нейтральными.

К ним относятся: *информация, коммуникация, конфликт, воздействие, угроза, опасность, безопасность, система*.

Термины этой группы отвечают требованиям однозначности и устойчивости, т.е. эти термины однозначно употребляются в одной области знаний и сохраняют свой особый смысл в каждой другой области знаний, а также являются общепризнанными – они употребляются в обиходе. Однако термину «информация» присуще специфическое свойство в разных областях знаний, и даже в одной области знания он может характеризовать предмет, явление, процесс и их свойства и отношения одновременно.

Термины, определяющие предметную основу информационной безопасности

Ко второй группе относятся термины, обозначающие понятия и их соотношение с другими понятиями в пределах информационной безопасности как специальной сферы или области знаний.

К таковым относятся: *информатика, информатизация, информационная система, информационные технологии, информационные процессы, информационный объект, информационный ресурс, информационная инфраструктура, информационная сфера, информационный потенциал*.

Термины, определяющие характер деятельности по обеспечению информационной безопасности

К третьей группе относятся термины, служащие обозначениями характерных для этой сферы предметов, явлений, процессов, их свойств и отношений (в том числе сил, средств и методов их использования при решении задач обеспечения информационной безопасности).

Термины этой группы обозначают широкий круг понятий различного уровня: от технического канала утечки информации до информационного противоборства.

К ним относятся: *информационное противоборство, информационное превосходство, информационная безопасность, угрозы информационной безопасности, обеспечение информационной безопасности, система обеспечения информационной безопасности, информационная защищенность, безопасность информации, защита информации, объект защиты информации, носитель информации, доступ к информации, доступность информации, целостность информации, конфиденциальность информации, несанкционированный доступ к информации, утечка информации, канал утечки информации, канал передачи информации, воздействие на информацию, информационно-психологическое воздействие, информационно-психологическая сфера.*

Важной специфической особенностью терминологической системы информационной безопасности является ее тесная связь с правовой лексикой. Это следствие того факта, что информационная безопасность давно перестала

быть технической дисциплиной, частью информатики. В связи с этим выработка единообразия в терминологии по проблеме обеспечения информационной безопасности создает предпосылки для целенаправленного развития всех работ по теории информационной безопасности и методологии защиты информации.

Предметной областью информационной безопасности являются:

- информация и ее свойства;
- угрозы безопасности информации и ее собственникам;
- политика безопасности и модели безопасности;
- способы, методы и средства защиты информации;
- классификация систем защиты;
- требования к защищенности информационных систем;
- методология оценки защищенности информационных систем и проектирования защиты;
- конкретные системы защиты информации, применяемые в различных органах управления, учреждениях и на предприятиях различных форм собственности.

Безопасность информации – защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Подходы к определению информационной безопасности

Сложность освещения проблемы обеспечения информационной безопасности связана с отсутствием до настоящего времени общепринятого толкования терминов, используемых для описания данной предметной области.

Н.В. Бекетов отмечает что, понятие «информационная безопасность» является сложным правовым явлением с точки зрения информационного права, поскольку вышеуказанную дефиницию следует рассматривать в праве как самостоятельный наднациональный вид всеобщей безопасности, поскольку на сегодняшний день информационное право затрагивает все сферы общественной жизни и обеспечивает развитие государства в целом.

В технической литературе информационная безопасность определяется через базовое понятие «безопасность». Следует отметить, что с одной стороны, безопасность рассматривается как состояние рассматриваемой системы (А.А. Малюк, В.И. Ярочкин), а с другой – как качество системы (А.А. Малюк, В.С. Горбатов и др.).

С точки зрения разработчиков технических систем использование первого похода к понятию не учитывает динамики изменений, происходящих в процессе функционирования системы.

Второй подход к понятию безопасности с позиций качества системы приводит к следующему определению информационной безопасности: «информационная безопасность системы – это ее качество, характеризующее,

с одной стороны, способность противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – уровень угроз, которые создает ее функционирование для элементов самой системы и внешней среды».

При таком определении мерой безопасности системы являются:

- с точки зрения способности противостоять дестабилизирующему воздействию внешних и внутренних угроз – степень (уровень) сохранения системой своей структуры, технологии и эффективности функционирования при воздействии дестабилизирующих факторов;
- с точки зрения отсутствия угроз для элементов системы и внешней среды – степень (уровень) возможности (или отсутствия возможности) появления таких дестабилизирующих факторов, которые могут представлять угрозу элементам самой системы или внешней среде.

Контекстное значение понятия «информационная безопасность» соответствует следующему смыслу:

- безопасность как свойство или способность системы не допускать опасных состояний, не переходить в них;
- безопасность как состояние системы, исключающее возможность опасного события и как условие протекания процесса, в котором исключается деструктивное воздействие на систему;
- безопасность как система мероприятий, обеспечивающих защиту системы от деструктивных воздействий (система обеспечения ИБ).

В соответствии с вышеизложенным, «информационная безопасность – это состояние защищенности жизненно важных интересов человека, общества и государства от угроз деструктивного воздействия в информационной сфере».

В основном определения понятия безопасности включают следующие основные положения: наличие внутренних и внешних угроз; наличие жизненно важных интересов и соблюдение баланса интересов. Первичным в определениях безопасности является наличие угроз и опасностей, далее – наличие жизненно важных интересов.

Отправными точками поиска путей в решении проблемы обеспечения ИБ могут служить:

1) информация как компонент АС и ее уязвимость;

2) особенности и структура информационного канала для объектов по аналогии с теорией информации Шеннона. Важнейшим моментом последнего является то, что характеристики полученного приемником (в том числе и биологическим объектом) информационного сигнала играют первостепенную роль и являются триггерами внутренних процессов.

Обеспечение ИБ в общей постановке проблемы может быть обусловлено при взаимосвязанном решении следующих задач:

- защите находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних информационных угроз;

- защите элементов ИС от дестабилизирующего воздействия внешних и внутренних информационно-полевых угроз;
- защите внешней среды от информационных угроз со стороны рассматриваемой системы.

Основные составляющие информационной безопасности

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Это свойство системы, в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. В связи с этим доступность выделяется как важнейший элемент информационной безопасности.

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. Это свойство информации существовать в неискаженном виде. Обычно интересует обеспечение более широкого свойства – достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, то есть ее неискаженности. Вопросы обеспечения адекватности отображения выходят за рамки проблемы обеспечения информационной безопасности.

Целостность можно подразделить на:

- статическую, понимаемую как неизменность информационных объектов;
- динамическую, относящуюся к корректному выполнению сложных действий. Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Конфиденциальность (секретность) – это защита от несанкционированного доступа к информации. Это субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации. Эта характеристика обеспечивается способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней. Объективные предпосылки подобного ограничения доступности информации

для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.

Для удовлетворения законных прав и интересов владельцев информации необходимо прежде всего постоянно поддерживать конфиденциальность (секретность), целостность и доступность информации. При нарушении хотя бы одного из этих свойств ценность информации снижается либо теряется вообще:

- если ценность теряется при ее раскрытии, то говорят, что имеется опасность нарушения секретности информации;
- если ценность информации теряется при изменении или уничтожении информации, то говорят, что имеется опасность для целостности информации;
- если ценность информации теряется при ее неоперативном использовании, то говорят, что имеется опасность нарушения доступности информации.

1.2. Государственное регулирование в сфере информационной безопасности Республики Беларусь

Информационная безопасность как составляющая часть национальной безопасности. Концепция информационной безопасности.

Обеспечение информационной безопасности в государственных программах.

Основные положения важнейших законодательных актов Республики Беларусь в области информационной безопасности и защиты информации.

Основные направления развития законодательства Республики Беларусь в сфере информационной безопасности.

В Республике Беларусь Указом Президента Республики Беларусь от 9 ноября 2010 г. №575 утверждена «Концепции национальной безопасности Республики Беларусь», которая определяет следующий понятийный аппарат:

национальная безопасность – состояние защищенности национальных интересов Республики Беларусь от внутренних и внешних угроз;

информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере;

национальные интересы – совокупность потребностей государства по реализации сбалансированных интересов личности, общества и государства, позволяющих обеспечивать конституционные права, свободы, высокое качество жизни граждан, независимость, территориальную целостность, суверенитет и устойчивое развитие Республики Беларусь. Основными национальными интересами в информационной сфере являются:

- реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;
- формирование и поступательное развитие информационного общества;
- равноправное участие Республики Беларусь в мировых информационных отношениях;
- преобразование информационной индустрии в экспортно-ориентированный сектор экономики;
- эффективное информационное обеспечение государственной политики;
- обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

источник угрозы национальной безопасности – фактор или совокупность факторов, способных при определенных условиях привести к возникновению угрозы национальной безопасности;

угроза национальной безопасности – потенциальная или реально существующая возможность нанесения ущерба национальным интересам Республики Беларусь.

В информационной сфере внутренними источниками угроз национальной безопасности являются:

- распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;
- зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;
- несоответствие качества национального контента мировому уровню;
- недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;
- рост преступности с использованием информационно-коммуникационных технологий;
- недостаточная эффективность информационного обеспечения государственной политики;
- несовершенство системы обеспечения безопасности критически важных объектов информатизации.

В информационной сфере внешними источниками угроз национальной безопасности являются:

- открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;
- доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;
- информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;
- нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;
- развитие технологий манипулирования информацией;
- препятствование распространению национального контента Республики Беларусь за рубежом;
- широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;
- попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

В информационной сфере с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации

прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг.

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

В 2019 году постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г №1 в Республике Беларусь была принята Концепция информационной безопасности, которой вводится в государственное правовое поле различные понятия с приставкой «кибер».

Данный документ определяет следующий понятийный аппарат:

кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз;

киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности;

кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти, либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка;

киберустойчивость – способность информационной системы предвидеть изменения обстановки и своевременно адаптироваться к ним в целях успешного предотвращения негативных последствий или быстрого восстановления после киберинцидента.

Указанный документ определяет, что целью обеспечения информационной безопасности является достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает

реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие.

Обеспечение информационной безопасности осуществляется в соответствии с государственной политикой в данной области, которая включает в себя формирование, совершенствование и реализацию организационных, правовых, научно-технических, правоохранительных, экономических мер обеспечения национальной безопасности в информационной сфере. В свою очередь, именно через развитие этой сферы главным образом обеспечивается и ее безопасность.

На государственном уровне осуществляется мониторинг, анализ и оценка состояния информационной безопасности, применяются индикаторы оценки ее состояния. Определяются приоритетные направления предотвращения угроз информационной безопасности, минимизации их деструктивного воздействия и локализации последствий. Разрабатывается и реализуется комплекс мер стратегического и тактического характера по предупреждению и нейтрализации информационных рисков, вызовов и угроз.

Государство всесторонне содействует защищенности национальных информационных систем, обеспечению безопасности используемого гражданами и организациями программного обеспечения. В целях улучшения устойчивости государственного сектора к информационным рискам осваиваются передовые технологии, внедряются новые средства и способы обеспечения информационной безопасности.

Разрабатываются стандарты информационной безопасности и с их учетом проводится аудит государственных систем информационной безопасности. Развивается смарт-проектирование решений по обеспечению информационной безопасности. На нормативном уровне выделяется и регламентируется функционирование критически важных объектов информатизации. Поощряется развитие технологий безопасности в бизнесе и жизнедеятельности граждан.

В Концепции информационной безопасности также определяется отдельным пунктом важность управления и менеджмент на государственном уровне рисками и угрозами в информационной среде, то есть способность адекватно и своевременно противодействовать кибератакам и возникающим киберинцидентам, а также их последствиям.

Государство осуществляет реагирование на риски и вызовы в информационной сфере в целях предупреждения их трансформации в угрозы национальной безопасности, развития и масштабирования вредоносного воздействия.

Реагирование на риски и вызовы в информационной сфере осуществляется всеми без исключения государственными органами и организациями в соответствии с областью их деятельности согласно непосредственному предназначению максимально полно и оперативно. Государство в лице этих государственных органов и организаций обеспечивает своевременное принятие мер безопасности, незамедлительно

оповещает заинтересованные субъекты, минимизирует ущерб и локализует последствия, определяет причастных лиц и организации, накапливает опыт противодействия угрозам.

Государственное реагирование на риски, вызовы и угрозы в информационной сфере предполагает сбор информации об используемых технологиях, способах деструктивных информационных воздействий и совершения киберпреступлений, анализ, оценку и прогнозирование состояния безопасности данной сферы, выявление реализующихся вызовов и угроз, локализацию негативных последствий и восстановление нанесенного вреда (ущерба). Определяется защищенность и устойчивость объектов информационной безопасности, в том числе информационной инфраструктуры, информационных ресурсов, индивидуального, группового и массового сознания к действию угроз. Выявляются и исключаются условия возникновения и реализации рисков, вызовов и угроз информационной безопасности.

Подготавливаются и внедряются сценарии и планы кризисного реагирования на кибератаки, компьютерные инциденты, акты деструктивного информационного воздействия, иные угрозы информационной безопасности, а также проводятся учения и тренировки сил реагирования.

Указанный документ определяет основные направления возникающих рисков и угроз информационной безопасности, концептуально рассматривает сферу кибербезопасности как новое направление для более подробного рассмотрения на государственном уровне в значительной степени связанное с информационной безопасностью, имеющее ряд подобий и отличительных черт.

В целях повышения уровня защиты национальной информационной инфраструктуры от внешних и внутренних угроз принят Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности».

В рамках данного Указа предусмотрено создание национальной системы обеспечения кибербезопасности, элементами которой являются:

- Оперативно-аналитический центр при Президенте Республики Беларусь;
- Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты;
- центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций;
- оператор электросвязи по взаимодействию Национального центра кибербезопасности, центров кибербезопасности, а также государственных органов и иных организаций;
- объекты информационной инфраструктуры государственных органов и иных организаций;
- сети передачи данных, используемые для взаимодействия элементов национальной системы обеспечения кибербезопасности.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

1.3. Международно-правовое регулирование в сфере информационной безопасности.

Подход НАТО к обеспечению кибербезопасности. Обеспечение кибербезопасности на уровне ООН. Конвенция Совета Европы о киберпреступности.

Положения кибербезопасности Европейского Союза. Обеспечение кибербезопасности в странах Европейского Союза.

Подход Соединенного Королевства в обеспечении кибернетической безопасности.

Обеспечение кибербезопасности Соединенных Штатов Америки.

Кибербезопасность и международное сотрудничество в киберпространстве Китайской Народной Республики.

Правовое регулирование информационной безопасности Российской Федерации.

Гармонизация законодательства стран СНГ по защите от преступлений и правонарушений в сфере информационной безопасности.

Информационные технологии приобрели трансграничный характер, а их эффективное применение становится фактором, который позволяет ускорить экономическое развитие страны, деятельности общества и отдельного индивидуума. Кроме того развитие технологий, их правильное использование способно совершенствовать работу общественных и государственных институтов. Неотъемлемой частью общественной и государственной жизни стал рост внедряемых информационных технологий во многих сферах: банковский сектор, СМИ, образование, транспорт, здравоохранение, энергетика, торговля, выделяется даже отдельный сегмент как «электронная торговля», жилищно-коммунальное хозяйство. При это как минимум пропорционально растет число киберугроз.

Отдельные страны рассматривают через призму кибербезопасности только неконтролируемое распространение в Интернете как всемирной системе объединенных сетей телекоммуникаций и вычислительных ресурсов электронных материалов, пропагандирующих терроризм, детскую порнографию и некоторые виды незаконной информации, в первую очередь, по причине технической сложности установления для них источника распространения такой информации.

Ряд стран в оценке угроз и принимаемых в отношении них мер противодействия придерживаются понятия информационной безопасности применительно ко всем аспектам использования ИКТ, выстраивая соответствующую модель правового регулирования и системы государственного управления.

Впервые руководители Североатлантического союза признали, что необходимо укреплять силы и средства в целях защиты от кибернетических нападений, на встрече на высшем уровне в 2002 году в Праге. С тех пор кибернетической проблематике стало уделяться все большее внимание в

повестках дня встреч **НАТО** на различных уровнях. В 2008 году были приняты первые основные принципы кибербезопасности НАТО. В 2014 году страны НАТО определили киберзащиту как одну из основных составляющих коллективной обороны, объявив, что в результате кибернетического нападения может быть приведено в действие положение о коллективной обороне, согласно (статье 5) основополагающего договора НАТО. В 2016 году страны НАТО обозначили кибернетическое пространство одной из сфер, в которых проводятся военные операции, и обязались в дальнейшем в приоритетном порядке укреплять кибербезопасность своих национальных сетей и инфраструктуры.

Руководство НАТО первым приняло ряд мер по исследованию, нормативному закреплению понятийного аппарата для деятельности в киберпространстве.

В частности, в НАТО используется определение, разработанное для Министерства внутренней безопасности США: «Кибербезопасность – это деятельность или процесс, способность, возможность или состояние, при которых системы связи и передачи информации, а также информация, содержащаяся в них, защищены и/или охраняются от вреда, несанкционированного использования, модификации или эксплуатации».

Краткое определение: деятельность или процесс, способность, потенциал или состояние, при котором информационно-коммуникационные системы и содержащаяся в них информация ограждены и (или) защищены от ущерба, несанкционированного применения, модификации или вторжения.

Расширенное определение: стратегия, политика и стандарты, регулирующие безопасность киберпространства и осуществляемых в нем операций и включающие в себя комплексную систему мер политики и мероприятий по снижению угрозы, уязвимости, сдерживанию, обеспечению международного взаимодействия, реагированию на инциденты, оптимизации потенциала для восстановления нормальной жизнедеятельности, включая проведение информационно-сетевых операций, обеспечение доступности, целостности и безопасности информации, реализацию правоохранительных и дипломатических мер, выполнение военных и разведывательных задач в части, относящейся к безопасности и стабильности глобальной инфраструктуры информации и средств связи.

В случае управления и регулирования сферой кибербезопасности в странах-членах НАТО принято выделять следующий пул проблем требующих управления и регулирования. При этом национальные рамки кибербезопасности могут иметь специфические различия, но в общем комплексный режим зачастую включает в себя следующие проблемы, нуждающиеся в активном урегулировании и координации:

- информационно-технологическое управление ресурсами;
- менеджмент контроля;
- конфигурация систем и конфигурация управления изменениями;
- идентификация и менеджмент уязвимостей;

- управление инцидентами;
- менеджмент непрерывности услуг;
- идентификация угроз и менеджмент решения проблем;
- внешние зависимости и менеджмент взаимосвязей;
- подготовка и информированность;
- поддержание владения ситуацией.

В области кибербезопасности создан Центр киберзащиты (CCD COE) (2008 год), как основная структурная единица по формированию подходов и методологии противодействия угрозам в киберпространстве, обучению персонала, выявлению и прогнозированию угроз, а также выработке и подготовке для руководства альянса концептуальных документов.

В НАТО также используются следующие термины:

Кибер-операция – использование кибер-возможностей для достижения цели в киберпространстве или с использованием него.

Кибератака – это кибер-операция, будь то наступательная или оборонительная, которая, с достаточной вероятностью, приведет к травме или смерти людей или повреждению или разрушению объектов.

В целом термин «кибербезопасность» и его производные (киберпространство, киберзащита, кибератаки, кибернападение и другие) не имеют единого общепризнанного юридического определения на международном уровне.

В тоже время на уровне **ООН** имеется ряд документов, таких как Глобальная программа кибербезопасности Международного союза электросвязи или Резолюция Генеральной Ассамблеи ООН «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур», в которых содержатся подходы к пониманию кибербезопасности, охватывающие сферу безопасного использования информационно-коммуникационных технологий в вопросах обеспечения:

1. неприкосновенности частной жизни;
2. конфиденциальности, целостности и доступности информации в электронной форме;
3. защиты критической информационно-коммуникационной инфраструктуры, взаимодействующей с Интернетом (в том числе информационных систем, аппаратно-программных комплексов, телекоммуникационных систем, сетей телекоммуникаций, систем защиты информации, программного обеспечения) от вредоносного воздействия программно-техническими методами.

Одним из основных документов для правового регулирования безопасности в информационной сфере является Всеобщая декларация прав человека. В данном акте закреплены гарантии на права и свободы человека и гражданина в части свободы убеждений, мысли, совести, религии, право на образование, а также право искать, получать и распространять информацию.

Кроме того, Всеобщей декларацией прав человека и конвенциями ООН дополнительно гарантированы права на частую жизнь.

В 1991 г. страны **Европы** разработали «Европейские критерии безопасности информационных технологий», которыми, в частности, определены задачи обеспечения информационной безопасности: защита информационных ресурсов от несанкционированного доступа с целью обеспечения конфиденциальности и целостности информационных ресурсов путем их защиты от несанкционированной модификации или уничтожения, а также обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

В 1996 г. стандарты европейской информационной безопасности были воплощены в «Единых условиях безопасности информационных технологий», согласно которым для характеристики основных критериев информационной безопасности применяется модель триады СИА (СИА TRIAD), которая предусматривает три основные характеристики информационной безопасности: конфиденциальность, целостность и доступность.

В 2001 г. была подписана Конвенция Совета Европы «О киберпреступности», которая и по сей день является одним из основных документов, регулирующих правоотношения в сфере глобальной информационной сети по предотвращению и контролю преступности, связанной с применением компьютеров. В Конвенции освещаются вопросы взаимодействия стран-членов Совета Европы в области обеспечения кибербезопасности.

В 2004 г. образовано Европейское агентство по сетевой и информационной безопасности (ENISA), координирующее деятельность стран союза для борьбы с киберугрозами.

Стратегия кибербезопасности ЕС, принятая в 2013 году, содержит следующие положения: предлагает расширение сотрудничества между государственными органами и частным сектором для противодействия трансграничным киберугрозам и координированию действий в чрезвычайных ситуациях; призывает государства-члены ратифицировать Будапештскую конвенцию Совета Европы о киберпреступности, и как можно скорее осуществить ее положения; в целях повышения устойчивости кибербезопасности информационных систем; в области обороны и национальной безопасности, предлагается, развитие потенциала кибербезопасности в области обнаружения, реагирования и противодействия киберугрозам; предлагается разработка основ политики ЕС в области кибербезопасности, в частности проработка учебных курсов по кибербезопасности и координация деятельности между международными партнерами, включая НАТО.

В 2016 году была согласована Директива Европейского Союза «О безопасности сетевых и информационных сетей», согласно которой государства-участники, должны гарантировать наличия национальных систем кибербезопасности, включающих:

1. Стратегии в области информационной безопасности, а также соответствующую политику и регулятивные меры, направленные на поддержание высокого уровня безопасности сетей и информационных систем;
2. Национальные уполномоченные органы для мониторинга реализации директивы на территории определенного государства и помощи по ее последовательной реализации;
3. Единого канала взаимодействия по вопросу безопасности сетей и информационных систем между государствами-участниками, группой взаимодействия и сетью групп реагирования на инциденты, связанные с компьютерной безопасностью;
4. Одной или нескольких групп, отвечающих за управление рисками и инцидентами.

Стратегия кибербезопасности **Германии** принята в 2011 г., направлена на предотвращение кибератак, уголовное преследование киберпреступлений, а также предупреждение выхода из строя физической составляющей информационных систем. Согласно стратегии ФРГ, кибербезопасность – это желаемое состояние кибербезопасности, при котором риски исходящие из киберпространства сведены к приемлемому минимуму.

В 2016 г. парламентом ФРГ был принят Закон «О кибербезопасности», дополняющий, изданную ранее стратегию кибербезопасности. Закон затрагивает вопросы обеспечения безопасности критической информационной инфраструктуры, в частности, согласно закону, поставщики информационных услуг обязаны в течение двух лет внедрить новые стандарты безопасности в киберпространстве.

Ведущую роль в обеспечении информационной безопасности в Германии играет Федеральная служба информационной безопасности (BSI). Согласно Закону «О Федеральном ведомстве безопасности информационных систем», BSI собирает и оценивает информацию относительно угроз кибербезопасности государства, обнаруживает новые типы кибератак, анализирует соответствующие контрмеры. Также на BSI во взаимодействии с НАТО и ЕС возлагается выполнение следующих функций: оценка риска внедрения информационных технологий; разработка критериев, методов и испытательных средств для оценки степени защищенности национальных телекоммуникационных систем; проверка степени защищенности информационных систем и выдача соответствующих сертификатов; выдача разрешений на внедрение информационных систем в важные государственные объекты; осуществление специальных мер безопасности информационного обмена; пропаганда необходимости обеспечения информационной безопасности.

В 2021 г. во **Франции** была принята Военная доктрина информационного влияния. Согласно документу, информационное противоборство будет дополнять оборонительные и наступательные действия Франции в киберпространстве, что обозначает проведение информационных акций по борьбе с террористической пропагандой и манипулированием информацией.

Национальная стратегия кибербезопасности **Австрии** использует более широкую концепцию безопасности ИКТ и рассматривает кибербезопасность как защиту систем ИКТ с помощью конституционных средств связанных с субъектом, технических, организационных и естественных опасностей, представляющих риск для безопасности киберпространства, включая инфраструктуру и безопасность данных, а также безопасность пользователей в киберпространстве.

В Австрийской стратегии приведена одна из наиболее полных классификаций киберугроз. Согласно матрице кибер-рисков, представленной в приложении к стратегии, киберугрозы условно можно разделить на 4 группы: маловероятные и неопасные; маловероятные и опасные; вероятные и неопасные; вероятные и опасные. Стоит отметить, что в стратегии кибербезопасности Австрии каждая киберугроза занимает свое определенное место в матрице рисков, по принципу системы координат, где ось X - вероятности возникновения киберугрозы, а ось Y – потенциальный ущерб от угрозы.

В стратегии кибербезопасности **Швеции**, которая была принята в 2016 году, под кибербезопасностью понимается комплекс мер безопасности, направленных на сохранение конфиденциальности, достоверности и доступности информации. Отличительной чертой шведской стратегии, является более подробное рассмотрение киберугроз, связанных с защитой суверенитета Швеции от внешнего посягательства.

3 октября 2019 года Комитет безопасности **Финляндии**, входящий в состав Министерства обороны, утвердил новую Стратегию кибербезопасности, обновляющую предыдущий документ от 2013 года. В стратегии обозначены три ключевых направления развития в области национальной информационной безопасности:

1. Развитие международного сотрудничества. Предполагает активное участие Финляндии в обсуждении вопросов кибербезопасности на площадках Европейского союза и ключевых международных организаций (ООН, ОЭСР, ОБСЕ, Совет Европы, НАТО).

Как отмечается в документе, Финляндия придерживается позиционируемого в Евросоюзе принципа атрибуции источника компьютерных атак и возможного применения в его отношении контрмер. Потенциальный ответ на угрозу может включать правоохранительные, дипломатические или активные меры в киберпространстве.

2. Улучшение координации при управлении кибербезопасностью.
3. Развитие компетентности (повседневных навыков) в сфере кибербезопасности.

Согласно данной стратегии, в основе обеспечения национальной кибербезопасности лежит принцип сотрудничества между властями, бизнес-сообществом, организациями и гражданами, когда каждый вносит свой вклад в общую безопасность.

Ключевую роль в обеспечении кибернетической безопасности **Польши** играет Агентство внутренней безопасности (ABW). В 2013 г. ABW разработало Стратегию кибербезопасности Польши и инициировало создание Центра криптологии при Министерстве национальной обороны, на который возложены задачи по защите информации, кибероборонны и проведения наступательных кибероперацій. ABW также создало правительственную команду реагирования на компьютерные инциденты (CERT), главной задачей которой является обеспечение и развитие возможностей органов государственного управления по защите от киберугроз, в частности, от атак на инфраструктуру, состоящую из IT-систем и компьютерных сетей, или разрушение которых может значительно угрожать жизни и здоровью людей, национальным богатствам.

Таким образом, в ряде стран таких как Франция, Чехия, Словакия применяется классическая модель обеспечения информационной безопасности, которая ориентируется на обеспечение и поддержание основных базисных принципов доступности, целостности и конфиденциальности информации.

Германия, Литва, Нидерланды в качестве ключевого элемента информационной и кибербезопасности определяют возможности по защите критически важных информационных систем и информационно-телекоммуникационных систем.

Страны, придерживающиеся политики нейтралитета: Австрия и Швейцария в своих подходах по обеспечению кибербезопасности акцентируют внимание на развитие международных возможностей по противодействию киберугрозам и уменьшения влияния преобладающих интересов нескольких стран в сфере ИКТ.

Подход **Соединенного Королевства** в обеспечении кибернетической безопасности направлен на развитие кибербезопасности как самостоятельной области. Цель: вывести Соединенное Королевство на первое место по инновациям, инвестициям и качеству сервисов в сфере информационно-телекоммуникационных технологий, и тем самым, в полной мере воспользоваться всеми преимуществами и достоинствами киберпространства. Значительные усилия принимаются по линии исключения рисков типа – кибератаки преступников, террористов и других государств с целью сделать киберпространство безопасным для граждан и экономики.

В Национальной стратегии кибербезопасности 2016-2021 указаны приоритеты наращивания суверенных возможностей для активных действий в целях защиты собственных интересов и криптографии.

Активная киберзащита – это принцип внедрения мер безопасности по усилению отказоустойчивости сети или системы перед атаками. В качестве целей активной киберзащиты обозначены:

- создание условий, в которых Соединенное Королевство станет гораздо более сложной мишенью для прогосударственных субъектов,

проводящих кибер-операции и кибер-преступников путем повышения устойчивости британских сетей;

- блокировка вредоносной коммуникации между хакерами и их жертвами, тем самым предотвращая работу вредоносных программ большой/малой сложности для активность в британских сетях;
- развитие и расширение возможности правительства по противодействию угрозам типа APT;
- укрепление критической инфраструктуры и гражданских сервисов перед различными типами киберугроз;
- нарушение используемых злоумышленниками бизнес-моделей путем создания экономической нецелесообразности ведения вредоносной активности в национальном пространстве и тем самым уменьшение вреда, который могут нанести их атаки.

Кроме того, в качестве приоритета определены: защита правительства от различных форм кибервоздействия, для чего повышается защищенность используемых сервисов, обучение задействованного персонала по пониманию киберугроз и принятию необходимых мер.

Правительство обеспечивает единый совместный подход к управлению инцидентами, основанный на улучшении понимания и осведомленности об угрозе и действиях, предпринимаемых против Соединенного королевства. Ключевым элементом управления и регулирования инцидентами и пониманием угроз является централизованный механизм НЦКБ, обеспечивающий партнерство с частным сектором, правоохранительными и другими государственными ведомствами, органами власти и агентствами, а также определяющий четкие процедуры отчетности об инцидентах с адаптацией к профилю жертвы.

Определяется приоритет укрепления навыков кибербезопасности и стимулирования роста в секторе кибербезопасности.

В сентябре 2018 г. Д. Трамп подписал Национальную киберстратегию **США**. Структурно она подразделяется на четыре направления: защита американского народа , Соединенных Штатов и американского образа жизни; (Protect the American People, the Homeland, and the American Way of Life); обеспечение процветания США (Promote American Prosperity); сохранение мира методом принуждения (Preserve Peace through Strength); продвижение американского влияния (Advance American Influence).

В первой части «Protect the American People, the Homeland, and the American Way of Life» обозначена цель – обеспечение надлежащего управления рисками в области кибербезопасности, повышение безопасности и защищенности информационных систем и информации, имеющей государственную важность .

Реализация цели первой части, происходит путем защиты федеральных сетей и информации, защиты критически важной инфраструктуры, борьбы с киберпреступностью и улучшения отчетности об инцидентах, включающей в себя предоставление департаменту внутренней безопасности более широких

полномочий контроля за гражданскими усилиями в области кибербезопасности, сотрудничество с другими странами в целях борьбы с киберпреступностью.

Приведенные в документе угрозы кибербезопасности США могут быть структурированы следующим образом: нарушение функционирования сетей федеральных департаментов и агентств; ненадлежащее качество IT продуктов и услуг в федеральной системе снабжения США; ненадежность федеральных подрядчиков, имеющих доступ к государственной тайне; использование государственными учреждениями устаревших IT продуктов или стандартов; дестабилизация критической инфраструктуры; кибератаки на избирательную инфраструктуру, транспортную, морскую и космическую инфраструктуру.

Вторая часть национальной стратегии кибербезопасности США – «Promote American Prosperity» ставит целью сохранить влияние Соединенных Штатов в технологической экосистеме и развивать киберпространство в качестве двигателя экономического роста, инноваций и эффективности.

Реализация цели второй части стратегии предполагает: развитие жизнеспособной и эффективной цифровой экономики; поощрение и защиту изобретательности США; создание квалифицированного кадрового резерва; сотрудничество с IT компаниями, для тестирования кибербезопасности в новых продуктах; привлечение и удержание высококвалифицированных кадров по кибербезопасности.

Во второй части киберстратегии представлен ряд мероприятий по обеспечению кибербезопасности США и международной безопасности, среди которых: создание единых международных стандартов кибербезопасности; создание стандартов кибербезопасности цифровой инфраструктуры следующего поколения; экономическая и политическая поддержка IT продуктов в сфере кибербезопасности американского производства; усиление контрразведывательных мероприятий в области IT технологий; финансирование программ школьного и университетского IT образования;

В третьей части «Preserve Peace through Strength» определена цель – «выявлять, противодействовать, пресекать, ослаблять интенсивность и сдерживать действия в киберпространстве, которые дестабилизируют и противоречат национальным интересам, сохраняя при этом превосходство США в киберпространстве и посредством него».

Осуществление данной цели предполагается посредством создания норм ответственного поведения государств и сдерживания недопустимого поведения в киберпространстве.

Четвертая часть «Advance American Influence» ставит целью сохранить долгосрочную открытость, функциональную совместимость, безопасность и надежность интернета, который поддерживается и усиливается интересами Соединенных Штатов.

Осуществление цели четвертой части стратегии, предполагает: продвижение открытого, международного, надежного и безопасного

Интернета; наращивание международного кибер-потенциала; совместное противодействие угрозам, направленным на взаимные интересы.

16 ноября 2018 года был подписал закон «Об Агентстве кибербезопасности и защиты инфраструктуры». Закон усиливает роль бывшего Национального управления по защите программам и преобразует его в агентство кибербезопасности и защиты инфраструктуры (CISA). Управлению предоставляются полномочия по созданию национального потенциала для защиты от кибератак и взаимодействию с федеральным правительством по предоставлению инструментов кибербезопасности, служб реагирования на инциденты и возможностей оценки для защиты государственных сетей.

7 ноября 2016 г. был принят Закон о кибербезопасности **КНР**. В документе закреплена обязанность государства обеспечивать «суверенность, безопасность и удовлетворение национальных интересов в киберпространстве». В законе дается определение ряду терминов, относящихся к сфере кибербезопасности. Согласно статье 76, кибербезопасность относится к принятию необходимых мер для предотвращения кибератак, вторжений, помех, уничтожения и незаконного использования, с целью обеспечения стабильной, надежной работы и конфиденциального функционирования сети. Сети рассматриваются здесь как системы, состоящие из компьютеров и других информационных устройств или объектов, используемых для «сбора, сохранения, передачи, обмена и обработки информации».

В статье 31 Закона о кибербезопасности КНР говорится, что государство должно сосредоточиться на вопросах защиты критической информационной инфраструктуры в сферах связи с общественностью, предоставления информационных услуг, энергетики, транспорта, водного хозяйства, финансов, государственных услуг, электронного правительства и других ключевых элементов информационной инфраструктуры, нарушение функционирования которой повлечет урон национальной безопасности, национальной экономике и поставит под угрозу жизни граждан.

Операторы критической информационной инфраструктуры должны хранить ключевые данные и персональную информацию на территории КНР. В тех случаях, когда необходимо предоставлять информацию внешним агентам, оценка безопасности проводится в соответствии с мерами, сформулированными национальным органом по управлению киберпространством совместно с соответствующими департаментами Государственного Совета. На операторов сетей возлагаются юридические обязательства в рамках закона.

Закон также устанавливает основополагающий принцип – поощрение и защита национального суверенитета в киберпространстве в рамках сетей. Перечень дополнительных обязательств для операторов сетей включает: соблюдение требований многоуровневой системы защиты кибербезопасности; аутентификацию реальной личности пользователей; разработку стратегий

действия в чрезвычайных ситуациях в области кибербезопасности; оказание помощи и поддержки следственным органам.

Также, закон регламентирует деятельность интернет СМИ и социальных сетей. Весь произведенный в сети контент сохраняется на территории КНР в течении 6 месяцев. Особое внимание в законе уделяется системе идентификации: для осуществления какой либо деятельности в сети, гражданам Китая необходимо подтвердить свою личность и пройти соответствующую процедуру верификации, иными словами, закон запрещает интернет анонимность.

Закон о кибербезопасности стал логичным продолжением проведения политики обеспечения контроля национального информационного пространства «Золотой щит», благодаря которой вероятность иностранного влияния на информационное поле внутри государства невысока.

В 2017 г. китайским правительством была утверждена Стратегия международного сотрудничества в киберпространстве. В документе закреплены следующие цели КНР: защита Интернет-суверенитета и невмешательство во внутренние дела суверенных государств; формирование системы международных правил в глобальном информационном пространстве; содействие установлению равноправного и справедливого участия государств в управлении Интернетом; защита законных прав и интересов граждан в киберпространстве; содействие международному сотрудничеству в цифровой экономике; создание платформ для обмена киберкультурой.

В Стратегии определен план реализации политики КНР на международной арене по достижению стратегической стабильности, установлению мира, выработке международных правил ответственного поведения государств в глобальном информационном пространстве, а также закреплены направления деятельности в области противодействия кибертерроризму и киберпреступности путем обмена опытом и технологиями с другими государствами.

Основы государственной политики **Российской Федерации** в области международной информационной безопасности (утверждены указом Президента Российской Федерации от 12 апреля 2021 г.№ 213). В документе подчеркивается необходимость заключения универсальных международно-правовых договоренностей, которые будут направлены на предупреждение конфликтов и выстраивание взаимовыгодного партнерства в мировом информационном пространстве при соблюдении незыблемости цифрового суверенитета государств.

Доктрина информационной безопасности Российской Федерации (утверждена указом Президента Российской Федерации от 5 декабря 2016 г. № 646) регулирует часть общественных отношений в информационной сфере, благодаря которым демонстрируется защищенность государства в информационной сфере и определяется дальнейшее совершенствование

правовых институтов с целью соблюдения баланса интересов личности, общества и государства в информационной среде.

В п. 8 Доктрины информационной безопасности РФ выделяются следующие особенности национальных интересов:

1) прозрачность и транспарентность деятельности государства в информационной сфере;

2) гарантия защиты конституционных прав и свобод граждан, касающихся информационной безопасности;

3) взаимное и согласованное функционирование государства и гражданского общества, в том числе в рамках укрепления нравственных ценностей общества;

4) обеспечение надлежащего функционирования информационной инфраструктуры как в случае непосредственного влияния информационных угроз (в том числе в военное время), так и в период стабильной мирной обстановки в стране;

5) стимулирование научно-технического прогресса и развития экономических отраслей, способствующих обеспечению информационной безопасности;

6) интеграционное взаимодействие с другими странами для обеспечения международной информационной безопасности и стратегической стабильности.

Национальные интересы в сфере информационной безопасности представляют собой общие ориентиры для органов публичной власти, на которых возложена роль нейтрализатора информационных угроз и конфликтов.

Среди перечня угроз информационной безопасности, к киберугрозам могут быть отнесены следующие:

1. Использование информационно-коммуникационных технологий, в частности сети-интернет, для обмена информации в военно-политических, криминальных, террористических и экстремистских целях;

2. Наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру Российской Федерации в военных целях;

3. Использование информационно-технических средств для разведывательных целей в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса;

4. Использование специальными службами иностранных государств средств информационно-психологического воздействия, направленного на дестабилизацию внутриполитической ситуации в различных регионах мира и России;

5. Кибератаки и иные виды компьютерных преступлений, связанные с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной

жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий;

6. Зависимость российской промышленности от зарубежных информационных технологий, недостаточный уровень развития конкурентоспособных отечественных информационных технологий.

26 июля 2017 г. был принят федеральный закон N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» который регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

В 2022 г. в **Узбекистане** был принят Закон о кибербезопасности, регулирующий отношения в этой сфере, а ранее, в 2005 г. и 2013 г. соответственно, были созданы Группа реагирования на чрезвычайные компьютерные ситуации и Центр информационной безопасности в рамках Государственного комитета по коммуникациям, развитию информационной системы и технологиям телекоммуникаций.

Законодательная база **Таджикистана**: Концепция информационной безопасности Республики Таджикистан (2003 г.) и Концепция государственной информационной политики (2008 г.), также приняты отдельные ведомственные законы, связанные с противодействием киберпреступности и насильственному экстремизму онлайн и оффлайн.

В **Кыргыстане**, основным документом, регулирующим связанную с ИКТ деятельность, является Концепция информационной безопасности Кыргызской Республики на 2019–2023 гг.

Ключевые приоритеты и понимание кибербезопасности в каждой стране национально значительно различается в зависимости от уровня развития ИКТ и экономики в целом. Следует отметить, что в отдельных странах приоритеты отдаются регулированию и обеспечению безопасности в отдельных сферах, созданию условий для работы бизнес сообщества и минимизации рисков и экономических потерь от кибератак и киберинцидентов. При этом кибербезопасность призвана обеспечить планомерное, а в некоторых случаях и ключевое функционирование экономики на современном уровне развития общества и роли технологий.

В связи с этим, различаются и подходы к составлению стратегий кибербезопасности, а также частота их пересмотров. Тем не менее, руководящие документы, охватывающие вопросы кибербезопасности, как правило, предусматривают:

- построение государственной системы управления в сфере обеспечения кибербезопасности;
- определение соответствующего механизма (в основном общественно-государственного партнерства), позволяющего частным и государственным заинтересованным сторонам обсуждать проблемы обеспечения безопасности национальных информационных инфраструктур;

⦿ определение необходимой политики безопасности и регулирующих механизмов, четкое обозначение ролей, прав и ответственности для частного и государственного сектора (например, обязательное информирование об инцидентах безопасности, базовые меры обеспечения безопасности и руководства к действию, новые нормы материально-технического обеспечения).

Как свидетельствует мировой опыт, полную защиту от ошибок в программном обеспечении или инцидентов информационной безопасности достигнуть невозможно, но путем осознанного ответственного поведения снизить их частоту и вероятность, обеспечить высокую скорость восстановления работоспособности информационных систем и ресурсов, чтобы не допустить разрушительных последствий, жизненно необходимо.

Координация этой сферы во многих странах в значительной степени выстраивается вокруг гражданского регулятора в области информационных технологий и связи (Агентство информационной безопасности KISA – Корея, Центр информационной безопасности Министерства информационных технологий – Республика Узбекистан), либо органа, ответственного за защиту и безопасность информации (Бюро безопасности информационной техники – Германия, Агентство безопасности информационных систем при Министерстве обороны – Франция, Агентство национальной безопасности Чехии, Федеральная служба безопасности и Федеральная служба по техническому и экспортному контролю Российской Федерации, в Европейском союзе регулятором в этой сфере является Агентство информационной и сетевой безопасности).

Таким образом, в киберпространстве различными странами в зависимости от проводимой внутренней и внешней политики, экономических приоритетов, уровня развития технологий, а также характерных угроз в киберпространстве применяются соответствующие подходы в регулировании и управлении кибербезопасностью. При этом за реализацию политики в указанной области могут отвечать специальные службы, министерство обороны и гражданские ведомства.

На сегодняшний день процесс формирования и развития международных норм в информационной сфере возникает по результатам межгосударственного сотрудничества в рамках международных организаций таких как ООН, Совет Европы, Европейский Союз, ШОС, БРИКС, ЕврАзЭС, СНГ, ОДКБ и других.

В рамках межгосударственного сотрудничества принимаются модельные законы об информационной безопасности, так на заседании Совета Парламентской Ассамблеи ОДКБ отдельно отмечено, что на данный момент всем странам-участницам необходимо усилить противодействие киберпреступности посредством внесения изменений в нормативные акты национального законодательства, в основе которого должен лежать модельный закон ОДКБ «Об информационной безопасности», принятый в 2021 г.

1.4. Угрозы информационной безопасности

Понятие и классификация угроз информационной безопасности. Источник угрозы - фактор (уязвимость) - угроза (действие) - последствия (атака). Классификация уязвимостей безопасности.

Внутренние и внешние угрозы.

Правовая защита от угроз воздействия информации на личность, общество и государство.

Под угрозой (в общем смысле) обычно понимают потенциально возможное событие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или непреднамеренными воздействиями на неё.

Под угрозой безопасности автоматизированных систем (АС) обработки информации понимается возможность воздействия на АС, которое прямо или косвенно может нанести ущерб ее безопасности.

Автоматизированная система является наиболее уязвимой частью информационной системы персональных данных, поскольку предоставляет злоумышленнику самый быстрый доступ к информации, в отличии от базы данных, хранящихся на бумажных носителях.

Моделирование и классификацию угроз и их проявлений, целесообразно проводить на основе анализа взаимодействия логической цепочки:

Источник угрозы → Фактор (уязвимость) → Угроза (действие) → Последствия (атака).

Источник угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Угроза (действие) [Threat]– это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.

Фактор (уязвимость) [Vulnerability] – это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

Последствия (атака) – это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).

Как видно из определения, атака – это всегда пара «источник – фактор», реализующая угрозу и приводящая к ущербу. При этом, анализ последствий предполагает проведение анализа возможного ущерба и выбора методов парирования угроз безопасности информации.

Угроза, как следует из определения, это опасность причинения ущерба, то есть в этом определении проявляется жесткая связь технических проблем с юридической категорией, каковой является «ущерб».

Проявления возможного ущерба могут быть различны:

- моральный и материальный ущерб деловой репутации организации;
- моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;
- материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;
- материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;
- материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;
- моральный и материальный ущерб от дезорганизации деятельности организации;
- материальный и моральный ущерб от нарушения международных отношений.

Ущерб может быть причинен каким-либо субъектом и в этом случае имеется налицо правонарушение, а также явиться следствием независящим от субъекта проявлений (например, стихийных случаев или иных воздействий, таких как проявления техногенных свойств цивилизации).

В первом случае налицо вина субъекта, которая определяет причиненный вред как состав преступления, совершенное по злому умыслу (умышленно, то есть деяние, совершенное с прямым или косвенным умыслом) или по неосторожности (деяние, совершенное по легкомыслию, небрежности, в результате невиновного причинения вреда) и причиненный ущерб должен квалифицироваться как состав преступления, оговоренный уголовным правом.

Во втором случае ущерб носит вероятностный характер и должен быть сопоставлен, как минимум с тем риском, который оговаривается гражданским, как предмет рассмотрения.

Необходимость классификации угроз информационной безопасности АС обусловлена тем, что хранимая и обрабатываемая информация в современных АС подвержена воздействию чрезвычайно большого числа факторов, в силу чего становится невозможным формализовать задачу описания полного множества угроз.

Поэтому для защищаемой системы обычно определяют не полный перечень угроз, а перечень классов угроз.

Основные угрозы воздействия информации на личность:

- угрозы конституционным правам и свободам человека и гражданина в информационной сфере:
- неправомерное ограничение доступа к открытым информационным ресурсам;
- нарушение конституционных прав и свобод граждан в области массовой информации;
- противоправное применение специальных средств воздействия на сознание;
- манипулирование информацией.

Основные угрозы воздействия информации на общество:

- неисполнение требований законодательства в области информационной сферы, создание монополии на формирование, получение и распространение информации;
- нарушение правил в области функционирования информационных систем (например, разработка и распространение программ, нарушающих нормальное функционирование информационных систем, внедрение электронных устройств для перехвата информации и т. д.);
- нарушение правил в сфере оборота информации;
- увеличение оттока за границу специалистов и правообладателей интеллектуальной собственности;
- усиление зависимости различных сфер жизнедеятельности общества от зарубежных информационных структур.

Основные угрозы воздействия информации на государство:

- разрушение единого информационного пространства государства;
- вытеснение национальных информационных агентств, СМИ и производителей средств информатизации с внутреннего информационного рынка;
- монополизация информационного рынка государства отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных СМИ по информированию отечественной и зарубежной аудитории,
- низкая эффективность информационного обеспечения государственной политики и др.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации:

1. Информационные угрозы:
   - несанкционированный доступ к информационным ресурсам;
   - незаконное копирование данных в информационных системах;
   - хищение информации из библиотек;
   - нарушение технологии обработки информации;
   - использование информационного оружия.
2. Программные угрозы:
   - использование ошибок и «дыр» в программном обеспечении;
   - компьютерные вирусы и вредоносные программы;

- установка «закладных» устройств.

3. Физические угрозы:

- уничтожение или разрушение средств обработки информации и связи;
- хищение носителей информации;
- хищение программных или аппаратных ключей средств криптографической защиты данных;
- воздействие на персонал.

4. Радиоэлектронные угрозы:

- внедрение электронных устройств перехвата информации в технические средства и помещения;
- перехват, расшифровка, подмена и уничтожение информации в каналах связи.

5. Организационно-правовые угрозы:

- закупки несовершенных или устаревших информационных технологий и средств информатизации;
- нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере.

Классификация возможных угроз информационной безопасности может быть проведена по следующим базовым признакам:

По природе возникновения:

- естественные угрозы, вызванные воздействиями на АС объективных физических процессов или стихийных природных явлений;
- искусственные угрозы безопасности АС, вызванные деятельностью человека.

По степени преднамеренности проявления:

- угрозы, вызванные ошибками или халатностью персонала, например: некомпетентное использование средств защиты, ввод ошибочных данных и т.п.;
- угрозы преднамеренного действия, например: действия злоумышленников.

По непосредственному источнику угроз:

- природная среда, например: стихийные бедствия, магнитные бури и пр.;
- человек, например: вербовка путем подкупа персонала, разглашение конфиденциальных данных и т.п.;
- санкционированные программно-аппаратные средства, например: удаление данных, отказ в работе ОС;
- несанкционированные программно-аппаратные средства, например: заражение компьютера вирусами с деструктивными функциями.

По положению источника угроз:

- вне контролируемой зоны АС, например: перехват данных, передаваемых по каналам связи, перехват побочных электромагнитных, акустических и других излучений устройств;

- в пределах контролируемой зоны АС, например: применение подслушивающих устройств, хищение распечаток, записей, носителей информации и т.п.;
- непосредственно в АС, например некорректное использование ресурсов АС.

По степени зависимости от активности АС:

- независимо от активности АС, например: вскрытие шифров криптозащиты информации;
- только в процессе обработки данных, например: угрозы выполнения и распространения программных вирусов.

По степени воздействия на АС:

- пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС, например: угроза копирования секретных данных;
- активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС, например: внедрение троянских коней и вирусов.

По этапам доступа пользователей или программ к ресурсам:

- угрозы, проявляющиеся на этапе доступа к ресурсам АС, например: угрозы несанкционированного доступа в АС;
- угрозы, проявляющиеся после разрешения доступа к ресурсам АС, например: угрозы несанкционированного или некорректного использования ресурсов АС.

По способу доступа к ресурсам АС:

- угрозы, осуществляемые с использованием стандартного пути доступа к ресурсам АС
- угрозы, осуществляемые с использованием скрытого нестандартного пути доступа к ресурсам АС, например: несанкционированный доступ к ресурсам АС путем использования недокументированных возможностей ОС.

По текущему месту расположения информации, хранимой и обрабатываемой в АС:

- угрозы доступа к информации, находящейся на внешних запоминающих устройствах, например: несанкционированное копирование секретной информации с жесткого диска;
- угрозы доступа к информации, находящейся в оперативной памяти, например: чтение остаточной информации из оперативной памяти, доступ к системной области оперативной памяти со стороны прикладных программ;
- угрозы доступа к информации, циркулирующей в линиях связи, например: незаконное подключение к линиям связи с последующим вводом ложных сообщений или модификацией передаваемых сообщений, незаконное подключение к линиям связи с целью прямой подмены законного пользователя с последующим вводом дезинформации и навязыванием ложных сообщений;

- угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере, например: запись отображаемой информации на скрытую видеокамеру.

Опасные воздействия на АС подразделяются на случайные и преднамеренные.

Причинами случайных воздействий при эксплуатации АС могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. В качестве нарушителя может быть служащий, посетитель, конкурент, наемник и т.д. Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой, сугубо материальным интересом (взятка), любопытством, конкурентной борьбой, стремлением самоутвердиться любой ценой и т.п.

Угрозы нарушения конфиденциальности направлены на разглашение конфиденциальной или секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ.

В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен несанкционированный доступ к некоторой закрытой информации, хранящейся в компьютерной системе или передаваемой от одной системы к другой.

Угрозы нарушения целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению.

Целостность информации может быть нарушена умышленно, а также в результате объективных воздействий со стороны среды, окружающей систему. Эта угроза особенно актуальна для систем передачи информации, компьютерных сетей и систем телекоммуникаций.

Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется полномочными лицами с обоснованной целью (таким изменением, например, является периодическая коррекция некоторой базы данных).

Угрозы нарушения доступности (отказ в обслуживании), направлены на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность АС, либо блокируют доступ к некоторым ее ресурсам.

Например, если один пользователь системы запрашивает доступ к некоторой службе, а другой предпринимает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании.

Блокирование доступа к ресурсу может быть постоянным или временным.

Эти виды угроз можно считать первичными или непосредственными, поскольку реализация этих угроз ведет к непосредственному воздействию на защищаемую информацию.

Основными угрозами информационной безопасности Республики Беларусь в общегосударственных информационных и телекоммуникационных системах являются :

1. Деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на осуществление контроля за функционированием информационных и телекоммуникационных систем;
2. Нарушение установленного регламента сбора , обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем , отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
3. Использование не сертифицированных в соответствии с требованиями безопасности средств и систем информатизации и контроля их эффективности;
4. Привлечение к работам по созданию ,развитию и защите информационных и телекоммуникационных систем организации и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности .

В кибепространстве в качестве основных источников угроз являются действия как специальных групп (специальных служб своих государств), распределенных групп злоумышленников (хакеров), предоставляющих в том числе услуги по атакам информационных систем и сетей, а также коммерческие «исследовательские» компании, создающие как «шпионское» программное обеспечение, так и оказывающие услуги по получению несанкционированного доступа.

Повсеместность использования современных компьютерных систем и способность осуществлять связь или взаимодействовать с помощью различных средств от мобильных устройств до носимых компьютеров создают для государственных и негосударственных субъектов ряд возможных векторов атак. Использование различных как логических, так и технических уязвимостей может привести к широким последствиям для национальной безопасности посредством таких намеренных действий, как шпионаж, снижение эффективности объектов командования и управления, кража интеллектуальной собственности и чувствительной информации личного характера, нарушение предоставление существующих услуг и

функционирования критически важной инфраструктуры или нанесение ущерба экономике и промышленности.

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны методы и средства шпионажа и диверсий, которые использовались и используются для добывания или уничтожения информации на объектах, не имеющих информационных систем. Эти методы также действенны и эффективны в условиях применения информационных систем. Чаще всего они используются для получения сведений о системе защиты с целью проникновения в информационную систему, а также для хищения и уничтожения информационных ресурсов.

К методам шпионажа и диверсий относятся:

- подслушивание;
- визуальное наблюдение;
- хищение документов и машинных носителей информации;
- хищение программ и атрибутов системы защиты; 60
- подкуп и шантаж сотрудников;
- сбор и анализ отходов машинных носителей информации;
- поджоги;
- взрывы.

1.5. Защита информации

Организация защиты информации. Средства реализации комплексной защиты информации. Правовые, организационные и технические меры защиты информации.

Основные принципы построения систем защиты. Функции защиты.

Эффективность защиты информации.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации – принятие правовых, организационных и технических мер, направленных:

1) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Замысел защиты информации – основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Объектом защиты информации является информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

Организация защиты информации – содержание и порядок действий, направленных на обеспечение защиты информации.

Система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Мероприятие по защите информации – совокупность действий, направленных на разработку и (или) практическое применение способов и средств защиты информации.

Техника защиты информации – средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели. Показатель эффективности защиты информации – мера или характеристика для оценки эффективности защиты информации. Нормы эффективности защиты информации – значения показателей эффективности защиты информации, установленные нормативными документами. Мероприятие по контролю эффективности защиты информации – совокупность действий, направленных на разработку и (или) практическое применение способов и средств контроля эффективности защиты информации.

Защита информации от утечки – деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Защита информации от несанкционированного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного доступа – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Защита информации от технической разведки – деятельность, направленная на предотвращение получения защищаемой информации разведкой с помощью технических средств.

Средства реализации комплексной защиты информации

Все средства защиты делятся на формальные (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и неформальные (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические.

Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Из наиболее известных аппаратных средств можно отметить схемы контроля информации по четности, схемы защиты полей памяти – по ключу и т.п.

Физические средства реализуются в виде автономных устройств и систем. Это могут быть, например замки на дверях помещений, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации. Считалось, что основными средствами защиты являются программные. Первоначально программные механизмы защиты включались, как правило, в состав ОС, управляющих ЭВМ, или систем управления базами данных. Практика показала, что надежность подобных механизмов защиты является явно недостаточной. Особенно слабым звеном оказалась защита по паролю. Поэтому в дальнейшем механизмы защиты становились все более сложными, с привлечением других средств обеспечения безопасности.

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы системы на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация).

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в данной стране или обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета и престижа человека.

Основные принципы построения систем защиты

Для защиты информации в информационных системах могут быть сформулированы следующие принципы:

1. Законность и обоснованность защиты.

Принцип законности и обоснованности предусматривает то, что защищаемая информация по своему правовому статусу относится к информации, которой требуется защита в соответствии с законодательством.

2. Системность.

Системный подход к защите информационной системы предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов: ·

- при всех видах информационной деятельности и информационного проявления; ·
- во всех структурных элементах; ·
- при всех режимах функционирования; ·
- на всех этапах жизненного цикла;
- с учетом взаимодействия объекта защиты с внешней средой.

3. Комплексность.

Комплексное использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

4. Непрерывность защиты.

Защита информации — это непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы, начиная с самых ранних стадий проектирования. Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы.

5. Разумная достаточность.

Создать абсолютно непреодолимую систему защиты принципиально невозможно: при достаточных времени и средствах можно преодолеть любую защиту. Следовательно, возможно достижение лишь некоторого приемлемого уровня безопасности. Высокоэффективная система защиты требует больших ресурсов (финансовых, материальных, вычислительных, временных) и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

6. Гибкость.

Внешние условия и требования с течением времени меняются. Принятые меры и установленные средства защиты могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровня защищенности средства защиты должны обладать определенной гибкостью.

7. Открытость алгоритмов и механизмов защиты.

Суть принципа открытости механизмов и алгоритмов защиты состоит в том, что знание алгоритмов работы системы защиты не должно давать возможности ее преодоления даже разработчику защиты. Однако это вовсе не

означает, что информация о конкретной системе защиты должна быть общедоступна, необходимо обеспечивать защиту от угрозы раскрытия параметров системы.

8. Простота применения средств защиты.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения малопонятных ему операций.

Функция защиты – совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в информационной системе различными средствами и методами в целях создания, поддержания и обеспечения условий, объективно необходимых для надежной защиты информации.

Полное множество функций защиты:

- ⦿ предупреждение возникновения условий, благоприятствующих появлению дестабилизирующих факторов;
- ⦿ предупреждение непосредственного проявления дестабилизирующих факторов;
- ⦿ обнаружение проявившихся дестабилизирующих факторов;
- ⦿ предупреждение воздействия на защищаемую информацию проявившихся дестабилизирующих факторов;
- ⦿ обнаружение воздействия дестабилизирующих факторов;
- ⦿ локализация воздействия дестабилизирующих факторов;
- ⦿ ликвидация последствий локализованного воздействия дестабилизирующих факторов.

2. ПРАКТИЧЕСКИЙ РАЗДЕЛ

2.1. Основные понятия и определения в области информационной безопасности

Вопросы к семинарскому занятию

1. Теория информационной безопасности.
2. Предметная область информационной безопасности и этапы развития.
3. Подходы к определению информационной безопасности.
4. Термины, определяющие научную основу информационной безопасности. Термины, определяющие предметную основу информационной безопасности. Термины, определяющие характер деятельности по обеспечению информационной безопасности.
5. Составляющие информационной безопасности: доступность, конфиденциальность, целостность, достоверность информации.
6. Проблемы информационной безопасности общества.

Темы рефератов

1. Предметная область информационной безопасности и этапы развития.
2. Подходы к определению информационной безопасности.
3. Составляющие информационной безопасности: доступность, конфиденциальность, целостность, достоверность информации.
4. Проблемы информационной безопасности общества.

2.2. Государственное регулирование в сфере информационной безопасности Республики Беларусь

Вопросы к семинарскому занятию

1. Информационная безопасность как составляющая часть национальной безопасности.
2. Анализ Концепции информационной безопасности Республики Беларусь.
3. Вопросы обеспечения информационной безопасности в государственных программах.
4. Основные положения важнейших законодательных актов Республики Беларусь в области информационной безопасности и защиты информации.
5. Основные направления развития законодательства Республики Беларусь в сфере информационной безопасности.

Темы рефератов

1. Информационная безопасность как составляющая часть национальной безопасности.
2. Вопросы обеспечения информационной безопасности в государственных программах.

3. Основные положения важнейших законодательных актов Республики Беларусь в области информационной безопасности и защиты информации.

4. Основные направления развития законодательства Республики Беларусь в сфере информационной безопасности.

2.3. Международно-правовое регулирование в сфере информационной безопасности

Вопросы к семинарскому занятию

1. Подход НАТО к обеспечению кибербезопасности.
2. Обеспечение кибербезопасности на уровне ООН.
3. Конвенция Совета Европы о киберпреступности.
4. Положения кибербезопасности Европейского Союза. Обеспечение кибербезопасности в странах Европейского Союза.
5. Подход Соединенного Королевства в обеспечении кибернетической безопасности.
6. Обеспечение кибербезопасности Соединенных Штатов Америки.
7. Кибербезопасность и международное сотрудничество в киберпространстве Китайской Народной Республики.
8. Правовое регулирование информационной безопасности Российской Федерации.
9. Гармонизация законодательства стран СНГ по защите от преступлений и правонарушений в сфере информационной безопасности.

Темы рефератов

1. Обеспечение кибербезопасности на уровне международных организаций.
2. Положения кибербезопасности Европейского Союза. Обеспечение кибербезопасности в странах Европейского Союза.
3. Подход Соединенного Королевства в обеспечении кибернетической безопасности.
4. Обеспечение кибербезопасности Соединенных Штатов Америки.
5. Кибербезопасность и международное сотрудничество в киберпространстве Китайской Народной Республики.
6. Гармонизация законодательства стран СНГ по защите от преступлений и правонарушений в сфере информационной безопасности.
7. Сотрудничество и перспективы развития взаимоотношений Республики Беларусь в сфере обеспечения информационной безопасности.

2.4. Угрозы информационной безопасности

Вопросы к семинарскому занятию

1. Понятие и классификация угроз информационной безопасности.
2. Источник угрозы - фактор (уязвимость) - угроза (действие) - последствия (атака).
3. Классификация уязвимостей безопасности.

4. Внутренние и внешние угрозы.
5. Правовая защита от угроз воздействия информации на личность, общество и государство.

Темы рефератов

1. Понятие и классификация угроз информационной безопасности.
2. Источник угрозы - фактор (уязвимость) - угроза (действие) - последствия (атака).
3. Классификация уязвимостей безопасности.
4. Внутренние и внешние угрозы.
5. Правовая защита от угроз воздействия информации на личность, общество и государство.

2.5. Защита информации

Вопросы к семинарскому занятию

1. Организация защиты информации.
2. Средства реализации комплексной защиты информации. Правовые, организационные и технические меры защиты информации.
3. Основные принципы построения систем защиты.
4. Функции защиты.
5. Эффективность защиты информации.

Темы рефератов

1. Организация защиты информации.
2. Средства реализации комплексной защиты информации. Правовые, организационные и технические меры защиты информации.
3. Основные принципы построения систем защиты.
4. Функции защиты.
5. Эффективность защиты информации.

3. РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ

Примерный перечень вопросов к зачету

1. Теория информационной безопасности.
2. Предметная область информационной безопасности.
3. Подходы к определению информационной безопасности.
4. Кибербезопасность.
5. Термины, определяющие научную основу информационной безопасности. Термины, определяющие предметную основу информационной безопасности. Термины, определяющие характер деятельности по обеспечению информационной безопасности.
6. Составляющие информационной безопасности: доступность, конфиденциальность, целостность, достоверность информации.
7. Кибербезопасность.
8. Проблемы информационной безопасности общества.
9. Информационная безопасность как составляющая часть национальной безопасности.
10. Внешние и внутренние источники угроз национальной безопасности в информационной сфере
11. Государственное реагирование на риски, вызовы и угрозы в информационной сфере.
12. Государственное регулирование в сфере информационной безопасности.
13. Концепция информационной безопасности Республики Беларусь.
14. Национальная система обеспечения кибербезопасности.
15. Обеспечение информационной безопасности в государственных программах.
16. Основные положения важнейших законодательных актов Республики Беларусь в области информационной безопасности и защиты информации.
17. Основные направления развития законодательства Республики Беларусь в сфере информационной безопасности.
18. Сотрудничество и перспективы развития взаимоотношений Республики Беларусь в сфере обеспечения информационной безопасности.
19. Международно-правовое регулирование в сфере информационной безопасности.
20. Подход НАТО к обеспечению кибербезопасности.
21. Обеспечение кибербезопасности на уровне ООН.
22. Конвенция Совета Европы о киберпреступности.
23. Положения кибербезопасности Европейского Союза.
24. Обеспечение кибербезопасности в странах Европейского Союза.
25. Подход Соединенного Королевства в обеспечении кибернетической безопасности.
26. Обеспечение кибербезопасности Соединенных Штатов Америки.

27. Кибербезопасность и международное сотрудничество в киберпространстве Китайской Народной Республики.

28. Правовое регулирование информационной безопасности Российской Федерации.

29. Понятие и классификация угроз информационной безопасности.

30. Источник угрозы - фактор (уязвимость) - угроза (действие) - последствия (атака).

31. Классификация уязвимостей безопасности.

32. Внутренние грозы информационной безопасности.

33. Внешние угрозы информационной безопасности.

34. Угрозы по способам воздействия на объекты информационной безопасности

35. Угрозы нарушения конфиденциальности, целостности и доступности информации

36. Правовая защита от угроз воздействия информации на личность, общество и государство.

37. Организация защиты информации.

38. Средства реализации комплексной защиты информации.

39. Правовые, организационные и технические меры защиты информации.

40. Основные принципы построения систем защиты.

41. Функции защиты информации.

42. Эффективность защиты информации.

4. ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ

4.1. Список рекомендуемой литературы

Основная

1. Акопян, А. Э. Методы обеспечения информационной безопасности / А. Э. Акопян, М. У. Кайтукова // Академическая публицистика. – 2021. – № 1. – С. 27-30.
2. Александрова, А. В. Информационная безопасность и конституционные права личности / А. В. Александрова, Е. И. Образумов // Наука. Общество. Государство. – 2021. – Т. 9. – № 1(33). – С. 63-70.
3. Арчаков, В. Ю. Нормативное регулирование информационной безопасности в Республике Беларусь (в условиях становления и развития цифровой экономики) / В. Ю. Арчаков, О. С. Макаров, А. Л. Баньковский // Право.by. – 2019. – № 1(57). – С. 84-89.
4. Основы информационной безопасности : учебное пособие для студентов вузов / Е. В. Вострецова. — Екатеринбург : Изд-во Урал. ун-та, 2019 — 204 с.
5. Теория информационной безопасности и методология защиты информации / Ю.А. Гатчин, В.В. Сухостат, А.С. Куракин, Ю.В. Донецкая. – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.
6. Данич, К. Н. Модели и методы обеспечения информационной безопасности в автоматизированных системах управления / К. Н. Данич, В. И. Воронов // Инновации. Наука. Образование. – 2021. – № 28. – С. 963-970.
7. Жаксыбекова, Е. А. Международная информационная безопасность в практике международных отношений / Е. А. Жаксыбекова // Евразийское Научное Объединение. – 2021. – № 1-5(71). – С. 391-393.
8. Камбулов, Д. А. Анализ потенциальных угроз информационной безопасности и обзор существующих методов защиты / Д. А. Камбулов // E-Scio. – 2021. – № 1(52). – С. 185-189.
9. Кириленко, В. П. Киберпреступность и цифровая трансформация / В. П. Кириленко, Г. В. Алексеев // Теоретическая и прикладная юриспруденция. – 2021. – № 1. – С. 39-53. – DOI 10.22394/2686-7834-2021-1-39-53.
10. Команов, П. А. Исследование безопасности смарт-контрактов Ethereum / П. А. Команов, Х. Ю. Ревазов, Д. А. Тавасиев // Международный научно-исследовательский журнал. – 2021. – № 1-1(103). – С. 80-83.
11. Комаров, П. В. Информационная безопасность. Определение, принципы / П. В. Комаров // Академическая публицистика. – 2021. – № 1. – С. 34-37.
12. Красовская, Н. Р. К вопросу о контроле фейков, дипфейков, фейковых аккаунтов в Интернете / Н. Р. Красовская, А. А. Гуляев // Вестник Удмуртского университета. Социология. Политология. Международные

отношения. – 2021. – Т. 5. – № 1. – С. 96-99. – DOI 10.35634/2587-9030-2021-5-1-96-99.

13. Кузина, Н. В. Психика и информационная безопасность в условиях пандемии: последствия для личности и государства / Н. В. Кузина // Galactica Media: Journal of Media Studies. – 2021. – Т. 3. – № 1. – С. 146-189.

14. Лыженкова, А. Н. Киберпреступления: понятие, классификация, юридическая ответственность, основные правила компьютерной безопасности / А. Н. Лыженкова, Т. Н. Шарыпова // Инновации. Наука. Образование. – 2021. – № 26. – С. 900-904.

15. Макаров, О. С. Системный взгляд на нормативное обеспечение информационной безопасности в Республике Беларусь / О. С. Макаров // Право и государство: теория и практика. – 2020. – № 8(188). – С. 124-129.

16. Макаров, О. С. Концептуальные направления правового регулирования в сфере информационной безопасности Республики Беларусь / О. С. Макаров, А. Л. Баньковский // Право.by. – 2018. – № 5(55). – С. 91-96.

17. Парамонов, А. В. Некоторые аспекты обеспечения национальной безопасности в информационной сфере / А. В. Парамонов, В. В. Харин // Актуальные проблемы государства и права. – 2021. – Т. 5. – № 17. – С. 161-170. – DOI 10.20310/2587-9340-2021-5-17-161-170.

18. Писаренко, Е. А. Актуальные проблемы государственного управления в сфере обеспечения безопасности современного информационного пространства: мировая практика / Е. А. Писаренко // Российское государствоведение. – 2019. – № 4. – С. 117-121.

19. Попов, В. Г. Классификация средств защиты информации в современных системах информационной безопасности / В. Г. Попов, Д. Ф. Галиаскаров // Научный электронный журнал Меридиан. – 2021. – № 3(56). – С. 142-144.

20. Редкоус, В. М. Об опыте законодательного обеспечения кибербезопасности на правовом пространстве СНГ / В. М. Редкоус // Закон и право. – 2022. – № 6. – С. 30-34.

21. Шарыпова, Т. Н. Анализ угроз информационной безопасности и способны ее защиты / Т. Н. Шарыпова, С. А. Селиванов // Наукосфера. – 2021. – № 1-1. – С. 242-245.

Дополнительная

22. Макаренко, С. И. Информационная безопасность: учебное пособие / С.И. Макаренко // СФ МГГУ им. М. А. Шолохова. – 2009 – 372 с.

23. . Конституция Республики Беларусь 1994 года (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г., и 17 октября 2004 г. и и 27 февраля 2022 г.) // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

24. Об информации, информатизации и защите информации : Закон Респ. Беларусь, 10 ноябр. 2008 г. № 455-З ; в ред. Закона Респ. Беларусь от

10.10.2022 г. // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

25. Об органах государственной безопасности : Закон Респ. Беларусь, 10 июля 2012 г. № 390-З ; в ред. Закона Респ. Беларусь от 17.07.2023 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

26. Об органе государственного управления в сфере цифрового развития и вопросах информатизации: Указ Президента Респ. Беларусь, 7 апреля 2022 г., № 136 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023

27. Об утверждении Государственной программы развития цифровой экономики и информационного общества на 2016-2020 годы : постановление Совета Министров Респ. Беларусь, 23 марта 2016 г. № 235 ; в ред. постановления Совета Министров Респ. Беларусь от 30.10.2020 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

28. Об утверждении Инструкции о порядке осуществления контроля технической защиты государственных секретов : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 29 июля 2013 г. № 48 : с изм. и доп., внес. приказом Оперативно-аналитического центра при Президенте Респ. Беларусь от 20.02.2020 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

29. Об утверждении Концепции национальной безопасности Республики Беларусь: Указ Президента Респ. Беларусь, 9 ноябр. 2010 г. № 575 : с изм. и доп., внес. Указом Президента Респ. Беларусь от 24.01.2014 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

30. Об утверждении Положения о порядке проведения государственной экспертизы средств технической и криптографической защиты информации: Приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 26 авг. 2013 г. № 60 ; в ред. приказа Оперативно-аналитического центра при Президенте Респ. Беларусь от 20.02.2020 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

31. Об утверждении соглашения между Правительством Республики Беларусь и Правительством Республики Казахстан о сотрудничестве в области защиты информации : постановление Совета Министров Респ. Беларусь, 01 сент. 2005 г. № 973 : с изм. и доп., внес. постановлением Совета Министров Респ. Беларусь от 12.07.2008 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

32. Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) : постановление Совета Министров Респ. Беларусь, 15 мая 2013 г. № 375: в ред. постановления Совета

Министров Респ. Беларусь от 12.03.2020 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

33. Об электронном документе и электронной цифровой подписи : Закон Респ. Беларусь, 28 дек. 2009 г. № 113-З: в ред. Закона Респ. Беларусь от 14.10.2022 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

34. О Государственной программе инновационного развития Республики Беларусь на 2016-2020 годы : Указ Президента Респ. Беларусь, 31 янв. 2017 г. № 31 ; с изм. и доп., внес. Указом Президента Респ. Беларусь от 07.07.2020 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

35. О Государственной программе «Цифровое развитие Беларуси» на 2021 - 2025 годы : постановление Совета Министров Респ. Беларусь от 02 февр. 2021 г., № 66 ; в ред. постановления Совета Министров Респ. Беларусь от 14.09.2023 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

36. О государственных секретах : Закон Респ. Беларусь, 19 июля 2010 г. № 170-З : с изм. и доп., внес. Законом Респ. Беларусь от 17.07.2023 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

37. О дебюрократизации государственного аппарата и повышении качества обеспечения жизнедеятельности населения : Директива Президента Республики Беларусь, 27 декабря 2006 г., № 2 : с изм. и доп., внес. Указом Президента Республики Беларусь от 13.06.2023 г. № 172 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

38. О кибербезопасности :Указ Президента Респ. Беларусь, 14 февр. 2023 г. № 40 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

39. О коммерческой тайне : Закон Респ. Беларусь, 5 янв. 2013 г. № 16-З : с изм. и доп., внес. Законом Респ. Беларусь от 17.07.2018 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

40. О Концепции информационной безопасности : Постановление Совета безопасности Респ. Беларусь, 18 марта 2019 г. № 1 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

41. О Концепции правовой политики Республики Беларусь: Указ Президента Респ. Беларусь, 28 июня 2023 г., № 196// Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

42. О Межведомственной комиссии по безопасности в информационной сфере: Указ Президента Респ. Беларусь, 16 нояб. 2017 г. № 413: в ред. Указа Президента Респ. Беларусь от 01.08.2022 г. // Эталон – Беларусь

[Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

43. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 (вместе с Положением о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, Положением о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации, Положением о порядке представления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации, Положением о порядке ведения Государственного реестра критически важных объектов информатизации) : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 20 февр. 2020 г.: в ред. приказа Оперативно-аналитического центра при Президенте Респ. Беларусь от 29.12.2022 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

44. О мерах по совершенствованию использования национального сегмента сети Интернет : Указ Президента Респ. Беларусь, 1 фев. 2010 г. № 60 ; в ред. Указа Президента Респ. Беларусь от 14.02.2023 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

45. О модельном законе «Об информации, информатизации и обеспечении информационной безопасности»: Постановление Межпарламентской Ассамблеи государств-участников СНГ, 28 нояб. 2014 г. № 41-15 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

46. О модельном Регламенте административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств-участников СНГ: Постановление Межпарламентской Ассамблеи государств-участников СНГ, 28 нояб. 2014 г. № 41-17 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

47. О некоторых вопросах в сфере государственных секретов : Указ Президента Респ. Беларусь, 25 фев. 2011 г. № 68 : с изм. и доп., внес. Указом Президента Респ. Беларусь от 03.06.2016 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

48. О некоторых вопросах развития информационного общества в Республике Беларусь (вместе с Положением о независимом регуляторе в сфере информационно-коммуникационных технологий) : Указ Президента Респ. Беларусь, 08 нояб. 2011 г. № 515 ; в ред. Указа Президента Респ. Беларусь от

22.06.2023 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

49. О некоторых вопросах совершенствования использования национального сегмента глобальной компьютерной сети Интернет (вместе с Положением о порядке государственной регистрации информационных сетей, систем и ресурсов национального сегмента глобальной компьютерной сети Интернет, размещенных на территории Республики Беларусь) : постановление Совета Министров Респ. Беларусь, 29 апр. 2010 г. № 644 : в ред. постановления Совета Министров Респ. Беларусь от 20.12.2019 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

50. О некоторых мерах по обеспечению безопасности критически важных объектов информатизации (вместе с Положением об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации): Указ Президента Респ. Беларусь, 25 окт. 2011 г. № 486: с изм. и доп., внес. Указом Президента Респ. Беларусь от 09.12.2019 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

51. О некоторых мерах по совершенствованию защиты информации (вместе с Положением о технической и криптографической защите информации, Положением о порядке отнесения объектов информатизации к критически важным объектам информатизации) : Указ Президента Респ. Беларусь, 16 апр. 2013 г. № 196: с изм. и доп., внес. Указом Президента Респ. Беларусь от 22.06.2023 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

52. О Парке высоких технологий: Декрет Президента Респ. Беларусь, 22 сент. 2005 г. № 12: с изм. и доп., внес. Указом Президента Респ. Беларусь от 12.04.2023 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

53. О подтверждении соответствия средств защиты информации: Приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 12 марта 2020 г. № 77; в ред. приказа Оперативно-аналитического центра при Президенте Респ. Беларусь от 28.12.2022 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

54. О порядке создания, развития и взаимодействия государственных цифровых платформ и государственных информационных систем: постановление Министерства связи и информатизации Республики Беларусь, 6 октября 2022 г., № 17 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

55. О приоритетных направлениях научной, научно-технической и инновационной деятельности на 2021 - 2025 годы : Указ Президента Респ. Беларусь от 07 мая 2020 г., № 156 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

56. О развитии Парка высоких технологий : Указ Президента Респ. Беларусь, 12 апр. 2023 г. № 102 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

57. О развитии цифровой экономики : Декрет Президента Респ. Беларусь, 21 дек. 2017 г. № 8 ; в ред. Декрета Президента Респ. Беларусь от 18.03.2021 г. // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

58. О ратификации Протокола о взаимодействии государств-членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере: Закон Респ. Беларусь, 15 июля 2015 г. № 292-З // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

59. О ратификации Соглашения между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности: Закон Респ. Беларусь, 04 янв. 2015 г. № 234-З // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

60. О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности : Закон Респ. Беларусь, 14 июля 2014 г. № 179-З // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

61. О Рекомендациях по совершенствованию и гармонизации национального законодательства государств-участников СНГ в сфере обеспечения информационной безопасности: постановление Межпарламентской Ассамблеи государств-участников СНГ, 23 нояб. 2012 г. № 38-20 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

62. О совершенствовании государственного регулирования в области защиты информации : Указ Президента Респ. Беларусь, 09.дек. 2019 г. № 449 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

63. О создании единой научно-информационной компьютерной сети : постановление Совета Министров Респ. Беларусь, 18 дек. 1997 г. № 1677 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

64. О стратегии развития информационного общества в Республике Беларусь на период до 2015 года и плане первоочередных мер по реализации Стратегии развития информационного общества в Республике Беларусь на 2010 : постановление Совета Министров Респ. Беларусь, 09 авг. 2010 г. № 1174 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

65. Соглашение о сотрудничестве государств - членов Организации Договора о коллективной безопасности в области обеспечения

информационной безопасности (Заключено в г.Минске 30.11.2017) : Указ Президента Респ. Беларусь, 27 апр.2018 г. № 149 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

66. О технической и криптографической защите персональных данных: Приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 12 ноябр. 2021 г. № 195 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

67. О типовых проектах законодательных актов МПА ЕврАзЭс в сфере информационных технологий («Об информатизации», «Об информационной безопасности», «Основные принципы электронной торговли») : Постановление Межпарламентской Ассамблеи государств-участников СНГ от 28 мая 2004 г. №5-20 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

4.2. Электронные ресурсы

1. Образовательный портал БГУ [Электронный ресурс]. – Режим доступа: http://dl.bsu.by. – Дата доступа: 12.09.2023.
2. Электронная библиотека БГУ [Электронный ресурс]. – Режим доступа: http://elib.bsu.by. – Дата доступа: 12.09.2023.