МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт машиностроения
(наименование института полностью)

Кафедра «Управление промышленной и экологической безопасностью»
(наименование кафедры)

20.04.01 Техносферная безопасность
(код и наименование направления подготовки, специальности)

Системы управления производственной, промышленной и экологической безопасностью
(направленность (профиль))

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему: Организация защиты информации в образовательной организации при возникновении чрезвычайных и аварийных ситуаций (на примере ФГБОУ ВО ТГУ)

Студент	И.А. Власов (И.О. Фамилия)	 (личная подпись)
Научный руководитель	Л.Н. Горина (И.О. Фамилия)	 (личная подпись)
Консультанты	И.Ю. Амирджанова (И.О. Фамилия)	 (личная подпись)

Руководитель программы д.п.н., профессор Л.Н. Горина (ученая степень, звание, И.О. Фамилия) _____ (личная подпись)

«_____»_____20__ г.

Допустить к защите
Заведующий кафедрой д.п.н., профессор Л.Н. Горина (ученая степень, звание, И.О. Фамилия) _____ (личная подпись)

«____» _____ 20___г.

Тольятти 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы настоящего диссертационного исследования определяется тем, что безопасность информационной инфраструктуры образовательного учреждения является обязательным условием и одним из критериев эффективности деятельности образовательного учреждения и обеспечения качества образования. При этом следует отметить отсутствие отраслевых методик действий по защите информации при возникновении внештатных ситуаций. Все это обусловило цель работы – разработку алгоритма организации системы защиты для обеспечения информационной безопасности на объектах инфраструктуры при возникновении чрезвычайных и аварийных ситуаций.

Обеспечение нормального функционирования образовательного учреждения в течение длительного промежутка времени требует обязательного учета возможности возникновения нештатных ситуаций различного типа и характера. Поэтому подготовка любого объекта к работе в условиях чрезвычайных ситуаций позволяет не только обеспечить должный уровень безопасности сотрудников и собственности образовательного учреждения, но и уменьшить влияние отрицательных воздействий.

Цель диссертационного исследования: анализ рисков возникновения внештатных ситуаций и их деструктивного воздействия на защищаемую информацию и инфраструктуру локальной вычислительной сети образовательной организации.

Объект диссертационного исследования: Тольяттинский государственный университет.

Предмет диссертационного исследования: инфраструктура сети, оборудования, информационных активов.

Задачи диссертационного исследования:

- изучить существующие решения;

- разработать методику защиты информации при возникновении чрезвычайных и аварийных ситуаций на примере ВУЗа.

Выбранный общенаучный метод исследования основан на предположении, что организация защиты информации в образовательном учреждении при опасности возникновения чрезвычайных ситуаций будет производиться более эффективно и качественно на основе оценки и анализа существующих рисков, если:

- рассмотрены подходы и методологические основания к исследованию информационной безопасности при возникновении ЧС;
- проанализированы риски возникновения ЧС и определены критерии их приемлемости;
- смоделирован алгоритм действий сотрудников при возникновении ЧС на основе имитационной модели угроз безопасности;
- проведена оценка эффективности применяемых средств защиты от воздействия деструктивных факторов;
- проведена работа по предупреждению и предотвращению чрезвычайных ситуаций на территории образовательного учреждения.

Практическая и теоретическая ценность работы состоит в повышении эффективности информационной безопасности при воздействии деструктивных факторов, оптимизация существующих средств и методик защиты, и, как следствие, обеспечение непрерывного доступа к информации при любых внешних воздействиях при сохранении ее целостности. При этом обеспечивается непрерывность бизнес-процессов при функционировании университета.

Во введении обосновываются актуальность и степень научной разработанности проблемы, определяются цель и задачи исследования.

В первом разделе приводятся понятия информационной опасности, информационной безопасности, информационной угрозы. Определяются факторы или совокупность факторов, создающих информационную опасность объектов и информационных активов университета.

Рассматривается физическая защита инфраструктуры от воздействий окружающей среды.

Рассматриваются экологические проблемы в структуре информационной безопасности, факторы информационно-психологического воздействия на сотрудников в условиях ЧС.

Второй раздел содержит определение опасности возникновения чрезвычайных и аварийных ситуаций и оценка их воздействия на информационную инфраструктуру.

Производится анализ существующих рисков, их оценка для дальнейшего совершенствования информационной безопасности, составляется модель угроз с последующими мерами нейтрализации рисков негативного воздействия. Рассматриваются методики прогнозирования ЧС.

Выводы являются основой оценки эффективности текущих мероприятий по оценке рисков информационной безопасности, связанных с возникновением внештатных ситуаций.

В третьем разделе описываются методика и проведение экспериментальных исследований, изучение и освоение теоретических моделей и физических характеристик оборудования систем жизнеобеспечения серверной комнаты, и влияние их на производительность серверного оборудования при изменяющихся параметрах, вызванных аварийными и нештатными ситуациями.

В заключении в обобщённом виде сформулированы выводы и рекомендации, полученные в ходе исследований.

Структура диссертации. Диссертация состоит из введения, разделов, заключения, списка используемых источников; основная часть изложена на 86 страницах; работа содержит 17 рисунков, 8 таблиц, 1 приложение.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем исследовании применены следующие термины с соответствующими определениями:

Информационная безопасность – практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные.

Гражданская оборона — система мероприятий по подготовке и защите населения, материальных и культурных ценностей от опасностей, возникающих при ведении военных действий или вследствие этих действий, а также при возникновении чрезвычайных ситуаций природного и техногенного характера.

ПЕРЕЧЕНЬ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

ИБ – информационная безопасность;

ГО – гражданская оборона;

ЧС – чрезвычайная ситуация;

СЗИ – система защиты информации;

КВИ – критически важная информация;

КВО – критически важные объекты;

КИО – каналы информационного обмена;

АСУ – автоматизированные системы управления;

ISACA – международная профессиональная ассоциация ИТ;

ФСТЭК – Федеральная служба по таможенному и экспортному контролю.

1 Информационная безопасность в условиях угрозы возникновения стихийных бедствий, чрезвычайных и аварийных ситуаций

1.1 Роль и задачи информационной безопасности в условиях возникновения ситуаций техногенного характера

Трудно переоценить роль информации и информационных технологий на современном этапе развития общества. Совокупность больших объемов данных, информационных объектов и управляющих структур представляет собой, по сути, интеллектуальный кластер модели социума и напрямую влияет на возникающие при этом общественные отношения. Владение и управление потоками информации может влиять на картину мира на геополитическом пространстве, и являются базисом управленческих решений руководителя любого уровне. Вместе с тем расширение границ информационных коммуникаций, изменения их структуры порождает и изменение взаимоотношений человека с информацией, проблемы на психологическом, этическом, экологическом и других уровнях. И избежать информационных рисков в связи с этим невозможно, но необходимо учитывать, оценивать и выстраивать систему защиты информации моделируя всевозможные ситуации деструктивного характера, как связанные с человеческим фактором, так и вызванные событиями естественного происхождения и возникающих чрезвычайных ситуаций.

Наиболее важными объектами в условиях чрезвычайных ситуаций является система управления и принятия решений в условиях развивающейся ситуации, ликвидации последствий деструктивных событий, система сбора, корреляции и обработки информации о возможности возникновения внештатных ситуаций или потоки данных от датчиков интегрированных систем в условиях развивающейся ситуации.

На сегодняшний день существует ряд макроподсистем обеспечения безопасности жизнедеятельности, реализуемых в пожарной и экологической

безопасности, в безопасности труда и т.п. А так как подсистемы имеют общую цель – противостоять угрозам техносферного характера, то становится актуальным вопрос интеграции макроподсистем путем взаимодействия по каналам связи с передачей данных, обработки их в автоматизированных вычислительных системах для организации комплексного управления техносферной безопасностью в промышленности, муниципальных образованиях. Важным дополнением к интегрированным системам являются программно-технические комплексы диспетчеризации и мониторинга событий безопасности для принятия управленческих решений и воздействия на объекты управления.

Наряду с обеспечением информационного обмена в едином информационном пространстве интегрированной среды встает вопрос обеспечения информационной безопасности, т.е. обеспечения целостности, доступности, конфиденциальности информации как в центрах обработки информации, так и при передаче по каналам связи.

При этом важно отметить, что на первый план выходит обеспечение целостности информации, т.е. неизменности данных при выполнении любых действий над ними, затем и доступности – обеспечение постоянного доступа к информационным ресурсам авторизованным пользователям систем, что особенно важно в условиях чрезвычайных и аварийных ситуаций [1].

Специфичными направлениями обеспечения информационной безопасности в вышеперечисленных условиях являются:

- обеспечение непрерывного и достоверного оповещения людей о событиях техногенного характера или чрезвычайной ситуации путем исключения подмены информации в коммуникационных сетях и проведение мероприятий по блокированию информационного воздействия и нейтрализации компьютерных атак;
- применение эффективной системы мониторинга объектов критически важной инфраструктуры, нарушение

функционирования которых может привести к возникновению ЧС или повлияет на возможность прогнозирования ЧС;

- внедрение мероприятий, обеспечивающих защиту информационных ресурсов КВО и систем прогнозирования ЧС, экологически опасных производств;
- повышение надежности передачи информации по каналам связи для принятия оперативных управленческих решений;
- проведение мероприятий направленных на нейтрализацию угроз информационно-психологического характера, подразумевающих изменение социально-психологического климата и манипуляторных воздействий на личность.

Важнейшим в рамках описываемой задачи является экологический аспект в информационной безопасности.

Согласно определению, предоставленному в [2], «Экологическая информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах, имеющих значение для охраны окружающей среды, обеспечения экологической безопасности, охраны здоровья граждан и так далее, независимо от формы их предоставления, освещение экологической ситуации в населенном пункте».

Нарушениями ИБ в экологической сфере являются утечки информации, кража и преднамеренное изменение данных, несанкционированный доступ с целью злонамеренных действий в информационных системах, навязывание ложной информации. Масштабы ущерба от подобных нарушений в экологической сфере могут быть огромными, т.к. напрямую касаются обеспечения безопасности жизнедеятельности граждан.

В общем, под угрозой информационной безопасности любой системы подразумеваются потенциально возможные действия или процессы, оказывающие деструктивное воздействие на систему или находящуюся в ней информацию. Принято различать естественные (воздействие объективных

природных или стихийных факторов) и внешние (присутствие человеческого фактора) угрозы. Угрозы первой группы наиболее опасны для информационной инфраструктуры, так как они влекут за собой наиболее негативные последствия. Ввиду физического разрушения систем информация утрачивается или становится недоступной. Помимо этого, имеют место сбои в работе компьютерных систем, недостатки в разработке аппаратных комплексов и наиболее опасное – умышленные или преднамеренные ошибки при разработке программного обеспечения, которые могут использоваться злоумышленниками в целях воздействия на ресурсы экологической системы.

При разработке комплекса мероприятий необходимо стремиться к минимизации последствий от аварий, стихийных бедствий, иных нештатных ситуаций. Это может быть достигнуто:

- обучением персонала действиям при внештатных ситуациях;
- правильным выбором месторасположения важных объектов при проектировании инфраструктуры;
- обеспечением резервных каналов электропитания и локальных сетей;
- резервным копированием важной информации с периодическим тестированием восстановления;
- разработкой и внедрением плана восстановления инфраструктуры;
- разработкой эффективной системы оповещения;
- использованием источников бесперебойного питания;
- использованием автоматических систем пожаротушения;
- обеспечением исключения несанкционированного доступа к КВО и КВИ;
- непрерывным мониторингом состояния КВО и целостности программной среды.

Данная методика была применена для обследования инфраструктуры университета с целью проверки соответствия указанным требованиям.

Были выявлены следующие несоответствия:

- прокладка некоторых трасс локальной вычислительной сети в подземных коммуникациях, которые частично затапливались сточными водами от ливневых дождей, что существенно снижало пропускную способность вплоть до полной потери связи;
- отсутствие мониторинга КВО и КВИ в режиме 7*24;
- отсутствие плана восстановления инфраструктуры после воздействия деструктивных ситуаций;
- отсутствие систем автоматического пожаротушения на КВО университета;
- неоправданно долгое по времени восстановление информации из резервных копий ввиду низкой технологичности используемой информационной системы;
- открытое, без использования специального кожуха, не защищенное расположение межэтажных кабельных переходов допускает несанкционированное подключение к ЛВС или умышленную порчу кабелей.

При этом необходимо отметить как правильные решения:

- расположение серверного помещения, исключающее затопление ввиду прорыва водопроводных трасс или систем отопления;
- обеспечение серверного помещения резервным каналом электропитания;
- оснащение серверного помещения системой пожароохранной сигнализации и оборудованием контролируемой зоны;
- обеспечением надлежащего контроля за вскрытием/закрытием объекта и исключением несанкционированного доступа.

Исходя из вышесказанного, можно дать определение информационной безопасности применительно условиям возникновения чрезвычайных и аварийных ситуаций: это обеспечение приемлемого уровня рисков возникновения деструктивных событий, при которых информационной инфраструктуре не будет нанесено существенного ущерба.

А информационной угрозой в этих же условиях будем считать совокупность событий представляющих информационную опасность инфраструктуре, приносящих существенный ущерб от источников техногенного характера.

1.2 Организация защиты информации в чрезвычайных и аварийных ситуациях

Возникшая стихийно чрезвычайная ситуация характеризуется слабым прогнозированием, а, следовательно, на предварительных этапах организации информационной безопасности для сохранения ее функционирования в чрезвычайных условиях принимаются меры общего характера, которые нацелены на сохранение жизни и здоровья сотрудников организации, а также на поддержание функционирования информационной инфраструктуры.

В настоящее время концепции управления безопасностью в организации системы защиты от чрезвычайных ситуаций непрерывно совершенствуются.

Это в частности:

- повышение качества подготовки и обучения персонала;
- совершенствование организации информационного обмена;
- усовершенствование качества прогностической основы управления;
- усиление вектора научных исследований задач управления информационной безопасностью в техногенной сфере;
- изучение и принятие экологических и психологических аспектов в оценке рисков;
- совершенствование процедур принятия управленческих решений.

Одной из наилучших практик управления ИБ по праву считается методика из зарубежного стандарта COBIT 5.

Факторы влияния, по отдельности и совместно, воздействуют на работоспособность чего-либо. В данном случае – на работоспособность руководства и управления ИТ на предприятии. Факторы влияния определяются каскадом целей, то есть высокоуровневые ИТ-цели определяют задачи для различных факторов влияния.

Методология COBIT 5 описывает семь видов факторов влияния, представленных на рисунке 1.

Рисунок 1 – Семь видов факторов влияния

- Принципы, политики и подходы обеспечивают трансляцию желаемого поведения в практические рекомендации по оперативному управлению.
- Процессы описывают структурированный набор практик и видов деятельности, необходимых для выполнения определенных задач и направленных на получение набора результатов, обеспечивающих достижение ИТ-целей.

- Организационная структура является важнейшей сущностью для принятия управленческих решений.
- Культура, этика и поведение людей и всей организации часто недооцениваются в качестве составляющей успешности руководства и управления.
- Информация повсеместно используется в любой организации и включает в себя всю информацию, производимую и используемую на предприятии. Информация требуется для того, чтобы организация работала и качественно управлялась, а на оперативном уровне информация зачастую является главным результатом деятельности организации.
- Услуги, инфраструктура и приложения включают в себя инфраструктуру, технологии и приложения, которые предоставляют инструменты обработки информации, а также услуги.
- Люди, навыки и компетенции необходимы для успешного выполнения всех видов деятельности, принятия правильных управленческих решений и выполнения корректирующих действий [3].

Организация защиты информации в чрезвычайных и аварийных ситуациях – непрерывный управленческий процесс, включающий в себя функционал управления:

- планированием;
- персоналом;
- инцидентами;
- чрезвычайными и аварийными ситуациями;
- событиями информационной безопасности.

Этот процесс схематически изображен на рисунке 2.

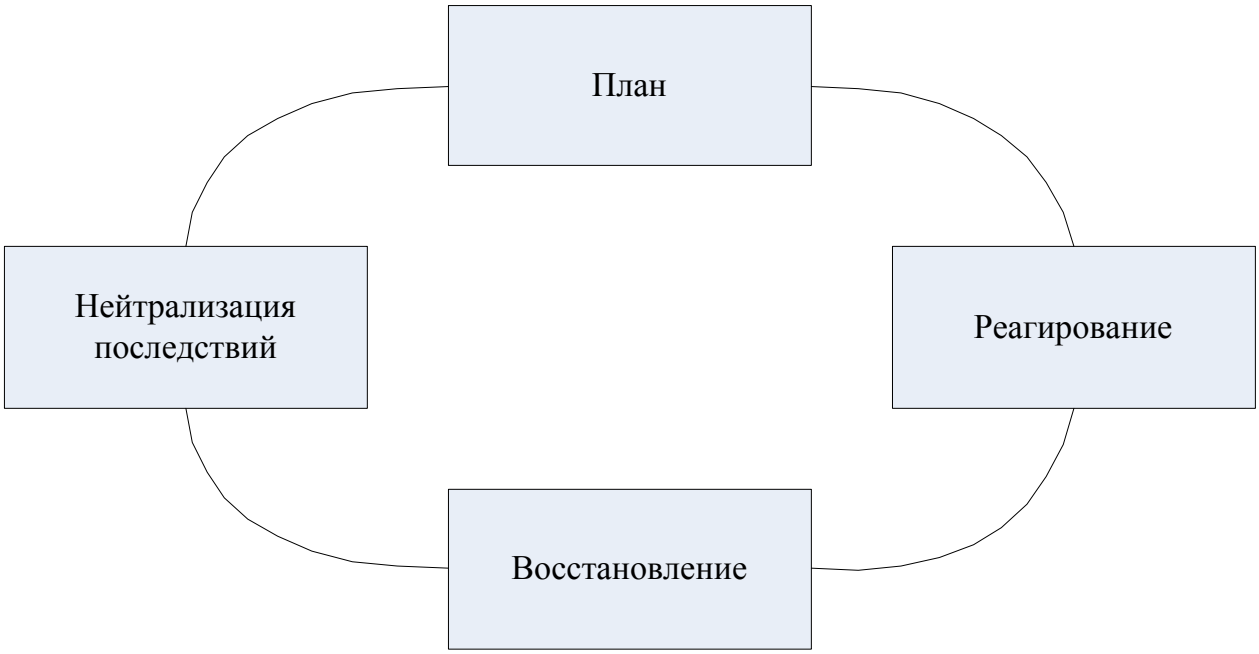

Рисунок 2 – Процесс управления ИБ

Прежде всего, рассмотрим виды угроз, вызываемые преднамеренными действиями или событиями, связанными окружающей средой, т.е. имеющими естественное происхождение.

Угрозы защищаемой инфраструктуры вызваны ее уязвимостью, т.е. ее неспособностью самостоятельно противостоять деструктирующим воздействиям, нарушающим ее целостность.

Угрозы, вызываемые преднамеренными действиями, обозначены в приводимой ниже таблице 1 буквой Д, угрозы случайными событиями (непреднамеренно совершаемые людьми) – буквой А и угрозы, имеющие естественное происхождение (не вызванные участием человека) – буквой Е.

Таблица 1 – Таблица угроз

Наименование угрозы	Д	А	Е
Затопление	+	+	+
Ураган			+
Землетрясение			+
Пожар	+	+	+
Удар молнии			+
Намеренное повреждение	+		

Наименование угрозы	Д	А	Е
Неисправности электроснабжения		+	
Неисправности водоснабжения		+	
Неисправности кондиционирования	+	+	
Броски напряжения		+	+
Запредельные величины температуры и влажности	+	+	+
Проникновение пыли			+
Воздействие электромагнитного излучения	+	+	+
Воздействие статического электричества	+	+	+
Несанкционированный доступ к инфраструктуре	+		
Биологические факторы (микробы, грызуны и т.д.)			+

В таблице 2 показаны риски воздействия деструктивных угроз на КВИ.

Таблица 2 – Риски воздействия деструктивных угроз на КВИ

Наименование угрозы	Серверная	Кабельные трассы	Рабочие места
Затопление		+	
Ураган			
Землетрясение	+	+	+
Пожар	+	+	+
Удар молнии		+	
Намеренное повреждение	+	+	+
Неисправности электроснабжения	+		+
Неисправности водоснабжения			
Неисправности кондиционирования	+		
Броски напряжения	+		+
Запредельные величины температуры и влажности	+	+	
Проникновение пыли	+		+
Воздействие электромагнитного излучения	+	+	+
Воздействие статического электричества	+	+	
Несанкционированный доступ к инфраструктуре злоумышленника или инсайдера	+	+	
Биологические факторы (микробы, грызуны и т.д.)		+	

Эти угрозы всесторонне рассматриваются и учитываются при разработке важнейших документов – плана восстановления инфраструктуры в случае событий чрезвычайного и аварийного характера. Речь идет о так называемом плане DRP (Disaster Recovery Plan) [4] и плана действий при возникновении внештатных и аварийных ситуаций.

Рассмотрим актуальность вышеперечисленных угроз для инфраструктуры университета для использования в дальнейшем при разработке плана DPR. При этом произведем расчет риска возникновения той или иной угрозы, влияющей на функционирование объектов. Для расчета данных используется формула

$$R = K/K(y), \quad (1.2.1)$$

где K – количество ситуаций данного типа в год;

K(y) – общее число свершившихся чрезвычайных ситуаций в год.

Полученные результаты сравниваются с частотой возникновения деструктивных ситуаций, и, в зависимости от последствий воздействия, определяется одна из трех групп риска: приемлемый, повышенный или неприемлемый.

Деструктивные ситуации и группы риска:

1) Затопление.

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- кабельные трассы;
- рабочие места пользователей при прорыве систем отопления и водоснабжения.

Методы предотвращения и прогнозирования:

- создание оперативных групп реагирования;
- обучение сотрудников групп действиям при аварийных ситуациях;
- мониторинг состояния объектов;

- создание контролируемых зон для КВИ;
- профилактические мероприятия;
- перенос кабельных каналов из подземных коммуникаций;
- расширение зон без проводного доступа;
- расположение КВО без систем отопления и водоснабжения.

R = 0. Риск приемлемый.

2) Землетрясение.

Актуальность – не актуально. Район не является сейсмологически активным.

3) Пожар.

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- все объекты инфраструктуры университета.

Методы предотвращения и прогнозирования:

- создание оперативных групп реагирования;
- обучение сотрудников групп действиям в случае пожара;
- мониторинг состояния объектов;
- создание автоматических систем пожаротушения для КВО;
- профилактические мероприятия;
- резервное копирование информации на отчуждаемые носители с хранением на трех объектах;
- создание резервного помещения хранения и обработки информации;
- интеграция противопожарных систем в комплекс системы разграничения доступа;
- поддержание систем пожарной сигнализации в исправном состоянии.

R = 0. Риск приемлемый.

4) Удар молнии.

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- кабельные трассы, оборудование, имеющее заземление.

Методы предотвращения и прогнозирования:

- создание оперативных групп реагирования;
- обучение сотрудников групп действиям во внештатных ситуациях;
- мониторинг состояния объектов;
- создание единого контура заземления;
- оборудование серверной дифракционной заземляющей решеткой;
- оборудование молниеотводов со шпилями;
- установка на открытых распределительных щитах стержневых молниеотводов;
- профилактические мероприятия.

R = 0. Риск приемлемый.

5) Намеренное повреждение.

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- все объекты инфраструктуры университета.

Методы предотвращения и прогнозирования:

- создание оперативных групп реагирования;
- обучение сотрудников групп действиям по восстановлению инфраструктуры;
- мониторинг состояния объектов;
- комплексная физическая защита инфраструктуры;
- обеспечение безопасности оборудования и каналов информационного обмена;

- обеспечение безопасности силовых и телекоммуникационных кабельных сетей;
- огласка результатов расследования инцидентов;
- использование дублирующих каналов;
- организация взаимодействия с правоохранительными органами.

R = 0. Риск приемлемый.

6) Неисправности электроснабжения.

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- все объекты инфраструктуры университета.

Методы предотвращения и прогнозирования:

- создание оперативных групп реагирования;
- обучение сотрудников групп действиям по восстановлению инфраструктуры;
- мониторинг состояния объектов;
- комплексная физическая защита инфраструктуры;
- обеспечение безопасности оборудования и каналов информационного обмена;
- обеспечение безопасности силовых и телекоммуникационных кабельных сетей;
- огласка результатов расследования инцидентов;
- использование дублирующих каналов;
- организация взаимодействия с правоохранительными органами.

За текущий год произошло 2 случая аварийного переключения цепей питания серверной на резервный источник питания.

R = 1. Риск повышенный.

7) Неисправности водоснабжения.

Актуальность – неактуально.

R = 0. Риск приемлемый.

8) Неисправности кондиционирования.

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- серверное помещение.

Методы предотвращения и прогнозирования:

- создание оперативных групп реагирования;
- обучение сотрудников групп действиям по восстановлению системы кондиционирования;
- мониторинг состояния системы кондиционирования;
- внедрение системы дистанционного контроля;
- обеспечение автоматического переключения на резервный канал электропитания;
- внедрение автоматизированной системы управления климатическими системами;
- использование дублирующих каналов;

За текущий год произошло 2 случая аварийной работы системы кондиционирования.

R = 1. Риск повышенный.

9) Броски напряжения.

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- все объекты сетевой инфраструктуры.

Методы предотвращения и прогнозирования:

- создание оперативных групп реагирования;
- установка нелинейных ограничителей перенапряжения;
- разноска элементов КВО по разным фазам электропитания;

- установка стабилизаторов и источников бесперебойного питания в серверной и распределительных шкафах;
- использование в электроснабжении серверной ограничительных реле и устройств защитного отключения;
- обеспечение автоматического переключения на резервный канал электропитания;
- использование дублирующих схем электроснабжения.

В течение года произошло 6 случаев перенапряжения в сети.

R = 1. Риск повышенный.

10) Запредельные величины температуры и влажности.

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- помещение серверной, подземные коммуникации кабель каналов.

Методы предотвращения и прогнозирования:

- создание оперативных групп реагирования;
- внедрение комплексной системы регистрации температурного режима в серверном помещении с автоматическим оповещением и регулированием вентиляции и кондиционирования на основе снятия показаний датчиков, установленных на КВО;
- постоянный мониторинг состояния температурного режима серверного помещения.

За текущий год произошло 2 случая аварийного повышения температурного режима.

R = 1. Риск повышенный.

11) Проникновение пыли.

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- рабочие места пользователей информационных систем.

Методы предотвращения и прогнозирования:

- периодическая профилактическая работа специалистов технического отдела.

R = 0. Риск приемлемый.

12) Воздействие электромагнитного излучения (ЭМУ).

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- все объекты сетевой инфраструктуры.

Методы предотвращения и прогнозирования:

- создание оперативных групп реагирования;
- определение и контроль существующих источников электромагнитного излучения;
- четкое категорирование объектов КВО чувствительных к воздействию ЭМУ;
- аттестация помещений на предмет защищенности к побочным ЭМУ;
- привлечение для работ на объектах КВО только сертифицированных специалистов;
- максимально возможное разнесение кабельных трасс между собой и относительно цепей электроснабжения и проводящих материалов;
- экранирование помещения;
- применение поглощающих материалов для напольного покрытия серверного помещения;
- применение специальных средств для ослабления электромагнитных полей;
- применение электромагнитного зашумления;
- в качестве линий передачи информации использование оптоволокна.

R = 0. Риск приемлемый.

13) Воздействие статического электричества.

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- все объекты сетевой инфраструктуры.

Методы предотвращения и прогнозирования:

- использование активного заземления при ремонте и обслуживании компьютерной техники;
- использования нейтрализаторов зарядов для серверного оборудования;
- мониторинг температуры и влажности в серверном помещении;
- использование мелкоячеистой сетки при проектировании или дооборудовании серверного помещения;
- привлечение для работ на объектах КВО только сертифицированных специалистов;
- применение установки для ионизации воздуха на КВО;
- экранирование и заземление помещений.

R = 0. Риск приемлемый.

14) Несанкционированный доступ (НСД) к инфраструктуре злоумышленником или инсайдером.

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- серверы, рабочие места, линии информационного обмена, коммуникационное оборудование.

Методы предотвращения и прогнозирования:

- обучение сотрудников групп оперативного реагирования обнаружению и локализации попыток или случаев НСД;
- внедрение и использования систем обнаружения вторжений;
- своевременное обнаружение и устранение уязвимостей;

- использование средств контроля DLP;
- мониторинг трафика с использованием ПО из группы NetFlow Analyzer;
- резервное копирование КВИ;
- мероприятия по противодействию фишингу;
- внедрение системы управления учетными записями и разграничения доступа, по возможности использование двухфакторной аутентификации для доступа к КВИ;
- внедрение, настройка контроля целостности программной среды и средств доверенной загрузки;
- выполнение мероприятий информационной безопасности при проведении ремонтно-восстановительных работ и обслуживании оборудования и оптимизации баз данных;
- противодействие использованию средств сетевой разведки, блокирование работы сканеров и любого активного трафика;
- использование защищенных каналов связи (VPN) и средств криптографической защиты.

В текущем году зафиксировано 3 инцидента, связанных с несанкционированным доступом в информационную систему.

R = 1. Риск повышенный.

15) Биологические факторы (микробы, грызуны и т.д.).

Актуальность – актуально.

Объекты инфраструктуры, подвергающиеся угрозе:

- кабельные трассы в подземных коммуникациях.

Методы предотвращения и прогнозирования:

- использование кабель каналов в металлическом исполнении;
- исключение подземной прокладки кабелей для передачи КВИ;
- прокладка изолированных кабелей в бетонных коробах.

R = 0. Риск приемлемый.

Целью планирования действий в нештатных ситуациях является минимизации отрицательных последствий деструктивного воздействия независимо от их масштаба.

В настоящее время фундаментального исследования проблем управления информационной безопасностью в естественно-техногенной сфере в источниках не описано, за исключением создания планов DRP в зарубежных методиках защиты информации и которые появляются в отечественной практике совсем недавно. Концепция создания подобного планирования на основе проведённых исследовательских процессов будет приведена во второй главе.

Также управленческие мероприятия по защите процессов обработки и хранения информации заключаются в разработке и планов действий при подготовке и эксплуатации систем защиты информации в чрезвычайных и аварийных ситуациях (Приложение А).

Управление персоналом, подготовка квалифицированных кадров, как было отмечено выше стоит на первых позициях. Это вызвано необходимостью проведения сложных мероприятий по разработке документации, прогнозированию, мониторингу и принятия важнейших оперативных управленческих решений.

Какими же компетенциями, исходя из выше изложенного, должен обладать специалист, занимающийся вопросами обеспечения информационной безопасности?

Прежде всего, вопросы кадровой безопасности относятся к самим специалистам по защите информации. Вопрос не праздный, так как для надлежащей организации защиты информации недостаточно иметь профильное образование. По оценкам многих экспертов в силу ряда причин выпускники не имеют тех знаний и навыков, которые востребованы у работодателей. Поэтому зачастую подобные должности занимают бывшие сотрудники силовых ведомств или ИТ-служб, хотя справедливо заметить, что

в последнее время акцент смещается на более молодые кадры, подготовленные в смежных областях деятельности. Итак, сотрудник ИБ, кто он?

Рисунок 3 – Компетенции сотрудника ИБ

На рисунке 3 представлены компетенции, которыми в идеале должен обладать специалист помимо специфических знаний и навыков в области ИБ для решения большинства задач защиты информации, а именно:

- ИТ – понимать работу операционных систем, программного обеспечения, для осуществления контроля за работой администраторов информационных систем и баз данных;
- Право – знать нормативную базу ИБ, отслеживать правоприменение законодательных актов, разрабатывать регламентирующие документы согласно законодательству;
- Комплексная безопасность – уметь организовать физическую безопасность контролируемых зон и критически важных объектов, работу в чрезвычайных и аварийных ситуациях, при стихийных бедствиях, работу с охранными структурами;

- Психология – умение работать с людьми, коммуникабельность, грамотное доведение задач ИБ до руководства на понятном языке, знать принципы социальной инженерии;
- Программирование – уметь работать с базами данных, получать необходимую системную информацию, недоступную в пользовательском режиме, писать скрипты различного назначения для программного инструментария специалиста по защите информации;
- Системное администрирование – знать сетевые технологии, принципы администрирования сетевых устройств для надлежащего контроля за работой системных администраторов и суперпользователей.

Интересна в этом плане аналитика от ISACA [5], представленная на рисунке 4, демонстрирующая каких навыков не хватает специалистам по защите информации, актуально и для нас.

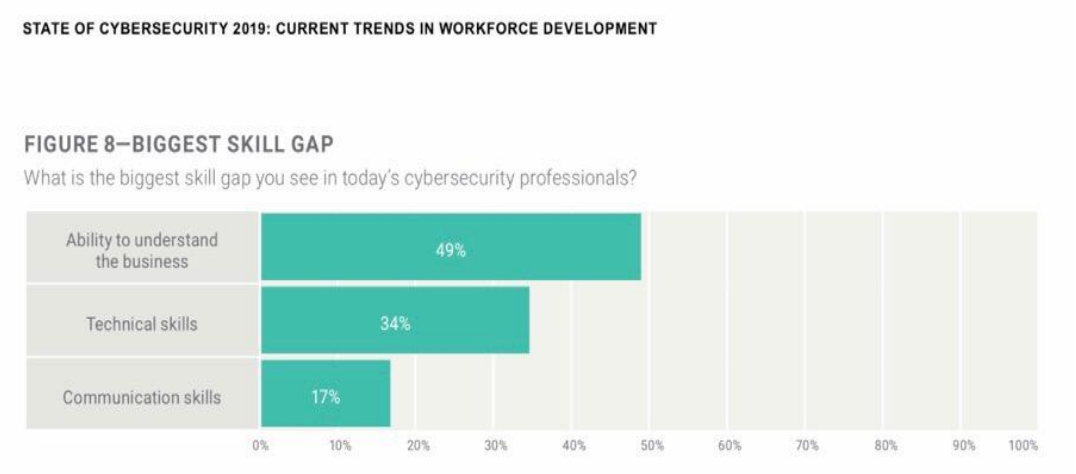

Рисунок 4 – Аналитика от ISACA

49 % – способность ИБ специалиста понимать задачи бизнеса (руководства), уметь разговаривать с ним на одном языке;

34 % – технические навыки по настройке аппаратных комплексов и средств защиты;

17 % – навыки коммуникации, уметь общаться с пользователями информационных систем и профильными специалистами.

Как правило, при приеме на работу специалиста по защите информации работник кадрового органа руководствуется квалификационными требованиями – профильное образование или техническое плюс курсы повышения квалификации по тематике информационной безопасности. На практике без систематического повышения квалификации, самообразования, участия в мероприятиях по ИБ этого недостаточно для большого спектра защиты информации.

Процесс управления чрезвычайными ситуациями схематично заключает в себе:

- разработку плана оперативного реагирования;
- определение групп лиц ответственных за реализацию плана оперативного реагирования;
- разработку и внедрение средств предупреждения, контроля и мероприятий по исключению несанкционированного доступа к объектам инфраструктуры в условиях отказов ее функционирования;
- осуществление координации действий службы информационной безопасности, охранного предприятия с мероприятиями по линии государственных правоохранительных органов и хозяйственных служб;
- мониторинг и анализ развивающейся ситуации, сопоставление уровня защиты с прогнозируемыми нарушениями;
- непрерывный контроль эффективности систем сигнализации, пожаротушения и оповещения;
- поддержание в готовности и исправности систем предупреждения о возникновении чрезвычайной ситуации;
- поддержание в дежурном режиме систем переключения на запасные каналы передачи информации;

- готовность к использованию резервных площадок обработки критически важной информации;
- контроль за состоянием защищенных каналов связи и средствами криптозащиты информации;
- обеспечение непрерывного контроля за исполнителями по выполнению инструкций на порядок действий при возникновения внештатных ситуаций;
- прогнозирование поведения сотрудников и студентов при доведении недостоверной информации о возможных чрезвычайных ситуациях и выработка мер по нейтрализации психологического воздействия в условиях этих ситуаций;
- выполнение процедур по восстановлению инфраструктуры после воздействия деструктивных событий.

Процесс управления инцидентами заключается в:

- обнаружении и распознавании атак и вторжений;
- реагировании на инцидент, локализация нападения;
- устранении последствий вторжения;
- восстановлении информации и инфраструктуры;
- идентификации нападающего;
- оценке и анализе атаки, выработке мер по предотвращению повторения схожего вектора атаки.

Таким образом, анализ и оценка инцидентов является посылом для реализации комплекса мер по совершенствованию информационной безопасности университета.

Заключительным этапом процесса управления инцидентами является устранение последствий нападения – локализация ущерба, причиненного вторжением. Подразумевается:

- смена паролей привилегированных пользователей или паролей доступа к скомпрометированным системам;

- переустановка операционных систем, а также программного обеспечения;
- восстановление параметров конфигурации оборудования и программного обеспечения;
- восстановление из бэкапов информационных систем и баз данных;
- блокирование вектора вторжения.

Кроме того, проводятся дополнительные мероприятия:

- работа с пользователями по повышению осведомленности;
- нейтрализация обнаруженных уязвимостей программного обеспечения;
- уведомление пользователей о произошедших инцидентах;
- передача сведений о компьютерной атаке группам реагирования на инциденты, определяемые приказом ФСТЭК.

Управление событиями информационной безопасности в режиме чрезвычайных ситуаций заключается в регистрации и анализе событий на сетевом оборудовании, системах оповещения, приложениях, выделении из логов подозрительных режимов работы и оперативном реагировании.

1.3 Методика расчета эффективности процессов защиты информации на критически важных объектах

Определив процессы управления информационной безопасностью в чрезвычайных и аварийных ситуациях оценим эффективность выстроенных процессов защиты, применяя методы математического анализа.

При проектировании системы защиты следует учитывать основное правило – степень защиты должна быть соразмерна с масштабом угроз. Только в этом случае можно говорить о действительной эффективности принимаемых мер.

За эффективность защиты информации условно принимается превышение времени преодоления защиты потенциальным злоумышленником над жизненным циклом информации [6].

Примем вероятность невозможности преодолеть систему защиты за $P_г$, время жизненного цикла информации за $T_ж$, ожидаемое время преодоления защиты злоумышленником $T_п$, вероятность преодоления преграды $P_р$, тогда для случая превышения жизненного цикла информации условие достаточности средств защиты будет следующим:

$$P_г = 1, \text{ если } T_ж < T_п \text{ и } P_р = 0, \quad (1.3.1)$$

Вероятность преодоления преграды равная нулю говорит о необходимости контура преграды вокруг объекта защиты.

Если $T_ж > T_п$, а $P_р = 0$, то $P_г = 1 - P_п$,

где $P_п$ – вероятность преодоления защиты за время меньшее $T_ж$.

Для случая, когда $T_ж > T_п$ и $P_п > 0$, прочность системы защиты (ПСЗ) выражается в следующем представлении:

$$P_г = (1 - P_п)(1 - P_р), \quad (1.3.2)$$

где $P_п = 0$, если $T_ж < T_п$; $P_п > 0$, если $T_ж >= T_п$.

При этом формальное значение прочности защиты будет соответствовать выражению (логическое выражение ИЛИ):

$$P_г = (1 - P_п) @ (1 - P_р), \quad (1.3.3)$$

Следовательно, эффективность защиты после сравнения значений $(1 - P_п)$ и $(1 - P_р)$ будет равна наименьшему значению одной из них.

В качестве примера защиты, рассчитываемого по формуле (1.3.3) возьмем криптографическую защиту информации, где значение переменной $P_п$ определяется оценкой вероятности установления кода ключевой формулы, с помощью которой можно расшифровать закрытую ключом информацию. Это значение можно получить по следующей формуле:

$$P_п = m / AC, \quad (1.3.4)$$

где m – число попыток подбора ключа;

A – число символов в строке кода ключа;

C – длина кода в символьной строке.

Значение $P_р$ зависит от примененного метода и алгоритма шифровки данных, применяемых методик крипто аналитик, применения

криптохранилищ, периодичности замены значения кода ключа, соблюдения политики обращения с закрытым ключом, иных обстоятельств, способствующих обходу криптозащиты.

Выбор и определение величины P_p проводятся, в том числе, экспертным путем на основе применения разработанных методик для данного типа алгоритма шифрования. Вероятность обхода криптозащиты злоумышленником принимает значения в диапазоне от 0 до 1.

Вполне вероятно, что у некой защиты может быть несколько путей обхода. Тогда формула (1.3.3) примет вид

$$P_r = (1 - P_n) @ (1- P_p)….@ (1- P_{pk}), \quad (1.3.5)$$

где к – число путей обхода защиты.

Эффективность защиты будет равна меньшему значению после определения и сравнения значений величин:

$$(1 - P_n), (1 - P_p), (1 - P_{pk}), \quad (1.3.6)$$

Если информационные процессы, как и сама информация, имеет длинные жизненные циклы и периодически обновляется, т.е. неравенство постоянно, или если обеспечить выполнение выражения (1.3.5) невозможно в силу причин, то применяют постоянную схему защиты, имеющую свойства обнаружения, блокировки вторжения в систему или на объект защиты. В качестве подобной схемы защиты физически выступает человек или при применении программно-аппаратного комплекса – система обнаружения вторжений (СОВ).

Параметры этой защиты будут влиять на ее эффективность.

Способность СОВ распознавать, обнаруживать и блокировать НСД должна учитываться при оценке ее эффективности путём введения в формулу (1.3.4) вместо $(1 - P_p)$ переменной P_o – вероятности обнаружения и заблокирования НСД.

Принцип работы СОВ состоит в постоянном опросе сенсоров (датчиков) в системных журналах (логах) средств защиты как дополнительного ПО, так и средств операционной системы или серверов.

Датчики, в свою очередь, это написанные скрипты для сбора и обработки информации предающейся и анализируемой ядром СОВ – программы управления. Периодичность опроса датчиков – тысячные доли секунды, что обеспечивает мгновенную передачу и анализ информации об аномальном поведении системы или подозрительном трафике. В этом случае время преодоления преграды злоумышленником значительно превышает время опроса сенсоров и обнаружения вторжения, поэтому такой контроль считается постоянным. При этом времени для обнаружения присутствия злоумышленника недостаточно, необходимо учесть также время на анализ информации с датчиков, которое значительно увеличивает временной интервал до принятия решения человеком (специалистом по безопасности).

На практике при возникновении подобного инцидента сразу блокируется сам факт доступа к объекту защиты, но в дальнейшем необходимо локализовать злоумышленника применением кейса средств и методов, что само по себе увеличивает время полной обработки инцидента.
Таким образом, условие эффективности защиты совместно с обнаружением и блокировкой НСД можно выразить следующим выражением

$$(t_d + t_c + t_m + t_b) / t_n < 1, \quad (1.3.7)$$

где t_d – период опроса сенсоров;

t_c – время срабатывания сигнализации;

t_m – время определения точки входа, t_b – время блокировки доступа злоумышленника.

Обозначив сумму $(t_d + t_c + t_m + t_b)$ как T получим отношение:

$$T / t_n < 1, \quad (1.3.8)$$

где T – время детектирования и блокировки НСД.

Отсюда следует, что злоумышленник может быть обнаружен в следующих случаях:

- если $t_n < T_i$;
- если $T_i < t_n < T$,

где T_i некий интервал времени между импульсами опроса сенсоров, поэтому в первом случае дополнительное условие – попадание t_n в интервал T – необходимость синхронизации действий нарушителя с периодичностью опроса сенсоров.

Задача технически очень сложная и по умолчанию принимается нерешаемой для злоумышленника, хотя некоторая вероятность успеха существует.

По определению геометрической вероятности выражение для определения вероятности успеха злоумышленника представлено в виде:

$$P_n = (T_i - t_n) / T_i = 1 - t_n / T_i, \quad (1.3.9)$$

при которой T_i – геометрическая мера, выражающая общее число всех возможных и равновозможных исходов данного испытания, а $(T_i - t_n)$ – мера, выражающая количество благоприятствующих событию n исходов.

Тогда вероятность обнаружения НСД будет определяться выражениями:

$$P_o = 1 - P_n$$

$$P_o = t_n / T_i, \quad (1.3.10)$$

При $t_n > T_i$ проникновение злоумышленника будет обнаружено с большой долей вероятности, т.е. $P_o = 1$.

Во втором случае вероятность проникновения будет определяться аналогично отношением:

$$P_n = 1 - t_n / T$$

Вероятность обнаружения и блокировки НСД:

$$P_o = 1 - P_n,$$

$$P_o = t_n / T$$

При $t_n > T$ попытка несанкционированного доступа не будет иметь смысла ввиду безусловной вероятности обнаружения, т.е. $P_o = 1$.

Исходя из вышеизложенного, эффективность защиты с функциями обнаружения и блокировки можно вычислять по формуле:

$$P_r = (1 - P_n) @ (1 - P_p)\ldots.@ (1 - P_{pl}), \quad (1.3.11)$$

где l – число обходов средств защиты информации.

Приведенная формула справедлива и для оранизационно-распорядительных мер защиты информации, выражающихся в периодическом мониторинге объектов защиты. Полагая, что детектирование и локализация НСД и его блокирование происходят одновременно – в период мониторинга событий на объектах защиты вероятность обнаружения инцидента будет определяться формулой (1.3.9).

Для более объективного представления эффективности системы защиты в виде системы обнаружения вторжений необходимо учитывать ее надежность и способы возможного преодоления злоумышленником.

Вероятность нарушения работоспособности системы определяется формулой:

$$P_{dist}(t) = e^{\mu t}$$

где μ – частота отказов элементов СОВ, t – интервал времени функционирования СОВ.

С учетом возможных отказов системы эффективность защиты определяется формулой:

$$P_r = P_o(1 - P_{dist}) @ (1 - P_p)\ldots.@ (1 - P_{pl}), \quad (1.3.13)$$

где l – число обходов средств защиты информации определяемых эмпирическим путем на основе анализа мониторинга средств защиты.

Одним из возможных способов обхода системы защиты является вмешательство злоумышленника в алгоритм работы СОВ, имитации вторжения, атаки на отказ в обслуживании и т.д. Вероятность подобных действий определяется эмпирическим путем от 0 до 1 на основе анализа работы СОВ.

На основании вышеизложенного можно сделать вывод, что защита от вторжений может быть контролируемой и управляемой, и не контролируемой. Эффективность защиты первой определяется по формуле (1.3.10), контролируемой по формуле (1.3.13). Но при использовании

автономных средств защиты расчеты эффективности следует производить по формуле:

$$P_r = P_{r1} @ P_{r2....} @ P_{ri} @ (1 - P_{p1}) @ (1- P_{p2}).…@ (1 - P_{pl}), (1.3.14)$$

где P_{ri} – эффективность защиты I-го уровня системы защищенности.

Для многоступенчатой защиты с контролируемой СОВ выражение будет иметь вид:

$$P_{rrn} = P_{rk1} @ P_{rk2....} @ P_{rkn} @ (1 - P_{p1}) @ (1 - P_{p2}).…@ (1 - P_{pl}), (1.3.15)$$

где P_{rkn} – эффективность защиты I-го уровня системы защищенности.

Итоговые расчеты должны быть раздельными, т.к. различаются задачи, следовательно, разные контуры защиты.

Если эффективность самого слабого элемента защиты удовлетворяет требованиям периметра защиты в целом, возможно говорить об избыточности уровня защищённости остальных элементов СОВ. Отсюда следует, что эффективнее применять на многоступенчатой защите элементы со схожими параметрами.

При расчете эффективности многоуровневой защиты возможно, что элемент с наименее значимыми параметрами не удовлетворяет требованиям. Тогда этот уровень дублируется или зеркалируется другими по эффективности элементами. Тогда суммарная прочность элементов защиты будет определяться формулой

$$P_{\sum} = 1 - \prod_{j=1}^{m}(1 - p(j)) , (1.3.16)$$

где j = 1,.., m – число дублирующих уровней защиты;

p(j) – эффективность защиты первого уровня.

Участок защитного контура с дублированными уровнями принято называть многоуровневой защитой.

В системе элементы защиты зачастую перекрывают друг друга и по ранее упомянутой причине, и тогда, когда особенности возможного вектора атаки требуют применения специфических средств защиты (например, СКУД, пожаро-охранной сигнализации, средств ограничения физического доступа). Это означает, что эффективность защиты p(j) попадающей в

область действия первого, второго, третьего уровня защищенности должна пересчитываться с учетом этих уровней по формуле (1.3.16). Соответственно может измениться и эффективность наименее слабого элемента системы.

При повышенных требованиях к защищенности информации применяется многоуровневая защита, что в университете реализовано в связке:

антивирус + IPTabels + МСЭ + Net Flow Analizator,

где IPTabels – СОВ;

МСЭ – межсетевой экран с ограничением трафика по портам;

Net Flow Analizator – анализатор входящего трафика с детектированием атак.

Модель многоуровневой защиты схематически представлена на рисунке 5.

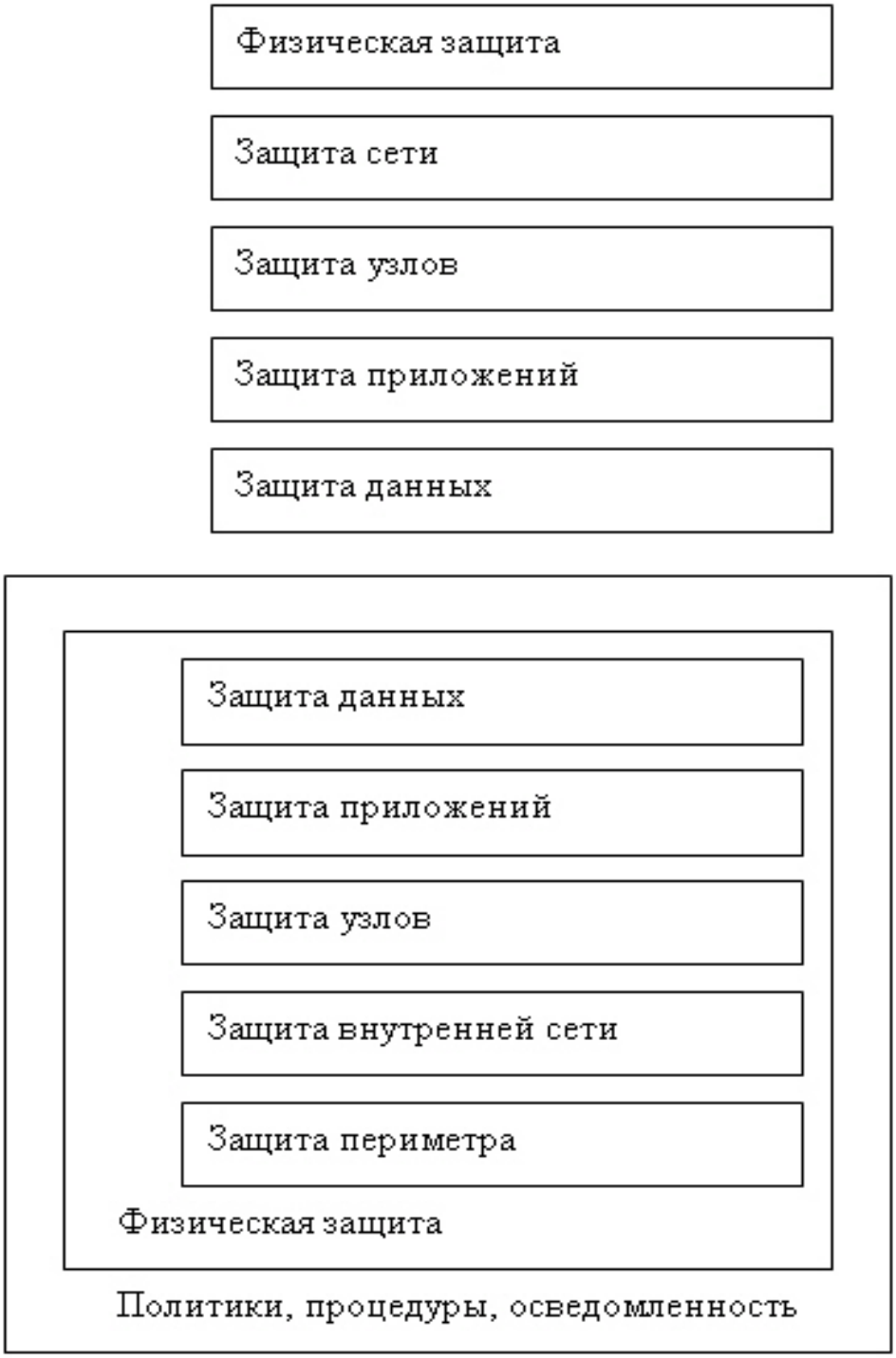

Рисунок 5 – Модель многоуровневой защиты

Вывод: Организацию системы управления информационной безопасностью необходимо разрабатывать на основе прогнозирования техногенных угроз, всесторонней оценки рисков и существующей системы защиты.

2 Разработка решения по совершенствованию уровня безопасности информационной инфраструктуры в условиях возможности ситуаций естественно-техногенного характера, аварий и катастроф

2.1 Модель рисков нарушений уровня информационной безопасности в условиях возможности наступления деструктивных событий.

Уровень защищенности информационной инфраструктуры организации обеспечивается приемлемым уровнем рисков нарушения информационной безопасности, т.е. угроз целостности, доступности и конфиденциальности информации. При угрозе возникновения чрезвычайных и аварийных ситуаций конфиденциальность уходит на второй план, а на первый – обеспечение целостности и доступности информационных ресурсов. В разработке организационно-распорядительной документации необходимо предусмотреть мероприятия по менеджменту рисков, алгоритм которого представлен в [7] и отражен на рисунке 6.

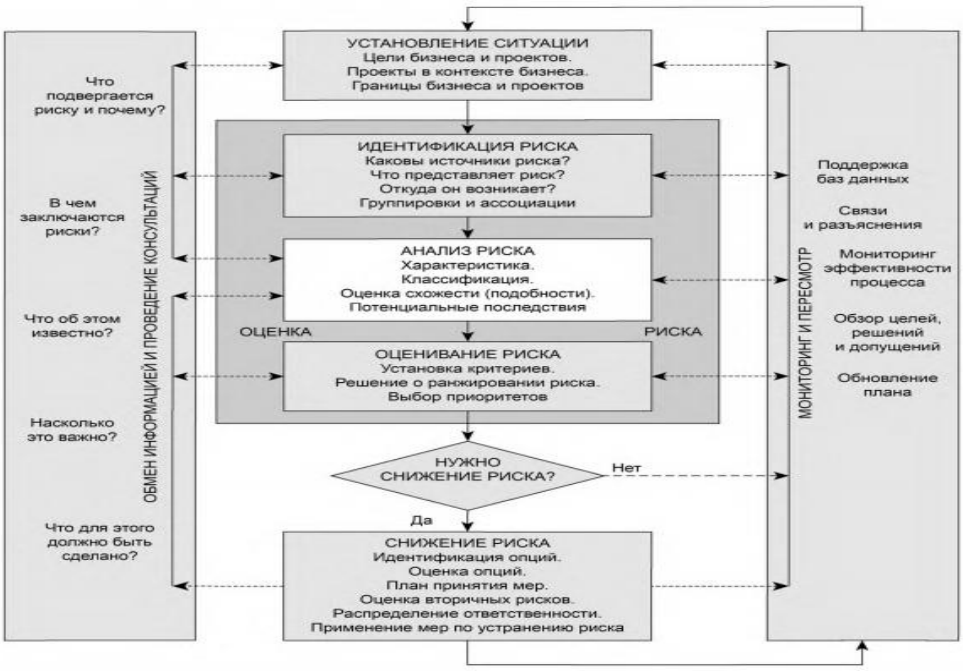

Рисунок 6 – Алгоритм менеджмента рисков

Нарушение доступности информации может произойти при возникновении следующих событий:

- сбой в работе аппаратных комплексов или программного обеспечения;
- компьютерная атака на информационные ресурсы со стороны внешних злоумышленников или инсайдеров;
- физическое уничтожение информационных ресурсов или инфраструктуры в целом в результате воздействия стихийных природных явлений или аварийных ситуаций.

Нарушение целостности информации помимо перечисленных выше событий может произойти в результате:

- умышленно занесённых программных закладок в программное обеспечение или конфигурацию системного ПО оборудования;
- установки технических средств разведок;
- подключения злоумышленниками дополнительного оборудования структуру локальной сети;
- сбоев в работе источников бесперебойного питания;
- непрофессиональных действий сотрудников при обслуживании и оптимизации баз данных информационных систем;
- нарушения условий поддержания оптимальных климатических условий для работы оборудования.

Классификация возможных масштабов деструктивных событий, определяемых в [8] приведена в таблице 3.

Таблица 3 – Классификация технических сбоев и катастроф

Уровень	Время простоя (часов)	Причина	Территория доступность	Число лиц, затронутых аварией	Воздействие на инфраструктуру
А	не > 2	Отказ нескольких рабочих станций	+	Не более пяти	Не значительное

Уровень	Время простоя (часов)	Причина	Территория доступность	Число лиц, затронутых аварией	Воздействие на инфраструктуру
B	не > 8	Отказ сервера, нарушение работы локальной сети	+	Более 10	Умеренное
C	не > 24	Затопление, длительное отключение энергии	_	Около 50% от численности	Значительное
D	> 24	Землетрясение, наводнение, пожар, террористический акт, война	_	Большинство	Критическое

Необходимым условием успешной разработки и внедрения плана мероприятий по восстановлению инфраструктуры после стихийных бедствий и чрезвычайных ситуаций является признание его необходимости руководством. Поэтому перед службой информационной безопасности стоит непростая задача аргументированного и убедительного доведения до руководителей организации актуальности плана, выделения финансовых средств для реализации. Помимо требований законодательства при этом, необходимо грамотно и на понятном руководству языке изложить и актуальные риски непрерывности бизнес процессов организации.

Немало важно показать и экономическую эффективность мероприятий, которая выражается не в получении прибыли от внедрения процессов, а от не упущения выгоды (штрафных санкций, затрат на восстановление разрушенной инфраструктуры, прерывания основной деятельности организации (в нашем случае учебного процесса)).

Одной из важных задач является выбор расположения резервного хранилища информации и обработки данных (резервная серверная). Необходимо предусмотреть при этом транспортную доступность, с одной стороны, и достаточную степень удаленности от основного кампуса с целью обеспечения независимости каналов электроснабжения и непопадания в зону поражения, с другой. На практике будем считать приемлемым расстоянием для перечисленных условий расстояние в 4-8 км. Меньшая удаленность не будет гарантировать сохранность резервной серверной при катастрофе, других стихийных бедствиях, а большая вызовет проблемы при реализации плана по факту возникновения катастроф или стихийных бедствий разрушительного характера.

Следующей по важности задачей является проведение аудита информационных ресурсов и определения кейса процессов обработки информации, необходимых для продолжения деятельности образовательного учреждения.

Очевидно, что вопросы целостности информации и связанные с этим мероприятия по обеспечению оцениваются в первую очередь. И самым простым и действенным способом сохранения целостности при любых возможных деструктивных воздействиях является организация резервного копирования и надежного хранения баз данных, копий конфигураций приложений, доменов, дисковых пространств. Данную задачу условно можно выполнить нижеследующими шагами:

а) Организация резервного копирования.

В первую очередь разрабатывается регламентирующий документ определяющий какие системы подлежат резервному копированию, в каком объеме, с какими временными интервалами, адреса хранения копий, ответственные за регламент копирования.

Выделяется отдельный сервер бэкапов, доступ к которому осуществляется по защищенному протоколу, например, ftp. Определяется приказом круг лиц, имеющих удалённый доступ к серверу. Физический

доступ должен быть только у системного администратора. Он же отвечает за разграничение доступа. Контроль доступа к серверу осуществляет специалист по информационной безопасности.

b) Определяются места хранения копий.

Копий бэкапов должно быть не менее трех и разнесены по разным помещениям территориально в разных зданиях. Хранение еженедельного архива, как вариант, осуществляется в арендованной банковской ячейке. Доступ к нему имеет только специалист по информационной безопасности.

c) Периодическое тестирование восстановление информации из архива.

Ввиду больших массивов данных в архивах восстановление может занимать большие отрезки времени. Поэтому периодичность процедуры тестирования устанавливается индивидуально для каждой системы, но не реже одного раза в три месяца.

Другим важным мероприятием является определение оптимального числа специалистов, необходимого для поддержания бизнес-процессов в восстановительный период. При этом надо признать возможность некоторого ослабления требований безопасности при выполнении восстановительных процедур (например, регламент вскрытия КВО, документирование процедур и т.д.). При этом сохраняется строгий контроль рисков нарушения двух других компонентов безопасности (доступности и целостности) и их увеличения до уровня неприемлемости. Работу специалистов по восстановлению технической инфраструктуры рекомендуется организовать в две смены.

2.2. Моделирование угроз безопасности в интегрированных автоматизированных системах управления техносферной безопасностью

Методика моделирования изложена в [1].

В силу специфичности с точки зрения информационной безопасности интегрированной АСУ выделим два наиболее важных информационных

актива – базы данных (БД) и каналы информационного обмена (КИО), которые будем рассматривать как объекты защиты от возможных угроз.

В БД на серверах аккумулируется и обрабатывается информация с систем мониторинга, данные с электро-баро-термо-акустических и т.п. датчиков, полученные по каналам связи, что предъявляет к ним требования обеспечения неизменности информации.

Моделирование угроз безопасности информации для рассматриваемых объектов предусматривает анализ способов несанкционированного доступа, изменения или уничтожения защищаемой информации с целью оценки рисков нанесения этими действиями ущерба. При моделировании угроз следует руководствоваться лучшими практиками [3, 9].

В нашем случае рассмотрим:

- моделирование физического проникновения к объектам защиты и воздействия окружающей среды;
- моделирование несанкционированного доступа к информации;
- моделирование угроз утечки информации по каналам связи и по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

2.2.1 Моделирование физического проникновения к объектам защиты и воздействия окружающий среды

При моделировании следует рассматривать:

- определение типа потенциального нарушителя (внешнего, внутреннего);
- предположения об имеющихся у нарушителя средствах атак для каждого типа нарушителя;
- предположения об имеющейся у нарушителя информации об объектах атак для каждого типа нарушителя;
- расположение контролируемых зон и их оборудование техническими средствами;

- систему охраны объектов;
- защиту объектов от физического проникновения;
- наличие охранной и аварийной сигнализаций;
- наличие устройств контроля доступа;
- расположение аварийных выходов, зон складирования и отгрузки материальных ценностей относительно контролируемых зон;
- расположение и защиту оборудования и средств хранения информации с учетом потенциальных угроз (воровство, задымление, пыль, вибрация, химические эффекты, электромагнитное излучение);
- наличие плана мероприятий ликвидации последствий от аварийного отключения электропитания, пожара, затопления или протекания воды через крышу, взрыва.

2.2.2 Моделирование несанкционированного доступа к информации

При моделировании следует рассматривать:

- защиту сетевых сервисов;
- наличие политик в отношении использования сетевых служб;
- наличие контроля маршрутизации;
- наличие контроля удаленного доступа и внешних соединений;
- сегментирование сети;
- наличие контроля фильтрации трафика с помощью определенных таблиц или правил;
- наличие контроля доступа к серверам на уровне операционной системы, регистрации событий безопасности;
- наличие мониторинга действий пользователей в системе;
- наличие контроля действий привилегированных пользователей;
- наличие политик Bring Your Own Device (BYOD, использование персональных устройств в рабочих целях);

- вероятность неумышленной (случайной) модификации (искажения) информации;
- вероятность преднамеренного уничтожения доступной информации;
- вероятность намеренного отключения средств защиты, внедрения вредоносных программ;
- наличие программ обнаружения (предотвращения) вторжений.

2.2.3 Моделирование угроз утечки информации по каналам связи

При интеграции территориально разнесенных подсистем одним из наиболее уязвимых участков являются каналы связи. Неизменность и целостность трафика является условием для принятия правильных управленческих решений, объективного отражения информации систем мониторинга и истинности управленческих сигналов на объекты воздействия.

Поэтому при моделировании угроз следует всесторонне оценить технические каналы связи по расположению, протяженности, защищенности от воздействий окружающей среды и физической недоступности, а также рассмотреть:

- возможность физического доступа к каналам связи;
- наличие контролируемого доступа к коммуникационным шкафам;
- коммутационные каналы, выходящие за пределы контролируемой зоны;
- системы электропитания, водоснабжения, канализации, силовые и телекоммуникационные линии и их расположение относительно каналов связи;
- возможность несанкционированного подключения к оконечному оборудованию;

- возможность скрытого снятия информации методами визуального наблюдения, акустического, оптического и электронного сканирования;
- наличие контроля подключения к узлам сети посторонних устройств;
- возможность утечки информации по каналам ПЭМИН.

В процессе составления модели угроз рассматривается вероятность реализации угроз. В дальнейшем по итогам оценки исходного уровня защищенности интегрированной системы и вероятности реализации угрозы (Y) рассчитывается коэффициент реализуемости угрозы и определяется возможность реализации угрозы, ее опасность и актуальность для построения системы защиты в целях нейтрализации актуальных угроз.

Под вероятностью реализации угрозы подразумевается определяемая условная величина, характеризующая, насколько вероятной является реализация описываемой угрозы для безопасности инфраструктуры в условиях теоретически рассматриваемой деструктивной ситуации.

Числовой коэффициент (Y3) для оценки вероятности реализации угрозы определяется по 4 показателям:

- маловероятно – отсутствуют объективные предпосылки условий для осуществления угрозы (Y3 = 0);
- низкая вероятность – предпосылки для реализации угрозы существуют, но планируемые мероприятия существенно затрудняют ее реализацию (Y3 = 2);
- средняя вероятность – объективные предпосылки для реализации угрозы существуют, но планируемые мероприятия обеспечения безопасности информационной инфраструктуры недостаточны (Y3 = 5);
- высокая вероятность – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности информационной инфраструктуры отсутствуют (Y3 = 10).

В рамках рассматриваемого вопроса выделим и оценим следующие угрозы:

1. Угрозы утечки информации по каналам ПЭМИН.

Угрозы утечки информации по каналу ПЭМИН возможны из-за наличия паразитных электромагнитных излучений у элементов ИС.

Угрозы данного класса маловероятны, т.к. ИС находится в пределах контролируемой зоны и её элементы находятся в центре здания и экранируются несущими стенами, паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в состав ИС.

2. Нарушение работоспособности технических средств.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИС и проходят каналы связи.

Охрана здания и контролируемой зоны осуществляется ЧОП «Арсенал» круглосуточно, в дневное время осуществляется контрольно-пропускной режим.

Доступ в серверную имеет строго определённый перечень лиц, утверждённый приказом ректора.

Вероятность реализации угрозы – маловероятна.

3. Вмешательство в работу (нарушение правил использования) средств защиты.

Угроза осуществляется путем НСД внешними и внутренними нарушителями к серверу.

Администраторы назначены из числа особо доверенных сотрудников. Охрана здания и контролируемой зоны осуществляется ЧОП «Арсенал» круглосуточно, в дневное время осуществляется контрольно-пропускной режим.

Доступ в серверную имеет строго определённый перечень лиц, утверждённый приказом ректора.

Вероятность реализации угрозы – маловероятна.

4. Угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления.

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности либо в результате стихийных бедствий.

В помещениях ИС установлена пожарная сигнализация, администраторы проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – маловероятна.

5. Сбой системы электроснабжения.

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В ИС осуществляется периодическое резервирование ключевых элементов ИС. Работают источники бесперебойного питания.

Вероятность реализации угрозы – маловероятна.

6. Возможность сбора информации нарушителем об объектах атак.

Угроза осуществляется вследствие несовершенства системы мониторинга и контроля, из-за чего может происходить НСД для сканирования хостов сети.

В ИС осуществляется мониторинг доступа на межсетевом экране (МСЭ) и анализ трафика на NetFow.

Вероятность реализации угрозы – маловероятна.

7. Угроза намеренного отключения средств защиты, внедрения вредоносных программ.

Угроза осуществляется вследствие отсутствия системы обнаружения вторжений, возможности повышения привилегий после проникновения, наличия административных полномочий у пользователей учебных подразделений.

В учебных подразделениях административные привилегии назначены только ответственным за ИБ. Внедрение вредоносных программ маловероятно при политике ограничения доверенной загрузки. Антивирус отключить невозможно при централизованном администрировании.

Вероятность реализации угрозы – маловероятна.

8. Угроза физического доступа к каналам связи, коммутационному оборудованию.

Угроза актуальна для доступа к оборудованию или каналам связи, кабельным линиям, находящимся вне контролируемых зон.

В университете локальная сеть прокладывается за потолочными панелями или в кабельканалах. Коммутационные шкафы закрыты, ключи у ответственных лиц, кабинеты сдаются под охрану, находятся в контролируемых зонах.

Вероятность реализации угрозы – маловероятна.

9. Угроза несанкционированного подключения к оконечному оборудованию.

Угроза актуальна для доступа к оборудованию, коммутационным шкафам, находящимся вне контролируемых зон.

В университете оконечное оборудование находится в контролируемых зонах. Коммутационные шкафы закрыты, ключи у ответственных лиц, кабинеты сдаются под охрану, находятся в контролируемых зонах. Ведется мониторинг подключения к ЛВС сторонних устройств. Имеется динамическая схема коммутационных устройств в виде веб-ресурса, показывающая в текущем режиме состояние коммутационных хостов.

Вероятность реализации угрозы – маловероятна.

По итогам оценки исходного уровня защищенности (Y2) и вероятности реализации угрозы (Y3), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы.

Коэффициент реализуемости угрозы Y будет определяться соотношением:

$$Y = (Y2 + Y3) / 20.$$

Оценка реализуемости УБ представлена в таблице 4.

Таблица 4 – Оценка реализуемости угроз безопасности

Тип угроз безопасности	Коэффициент реализуемости угрозы (Y)	Возможность реализации
Угрозы утечки информации по каналам ПЭМИН	0,4	низкая
Нарушение работоспособности технических средств	0,6	средняя
Вмешательство в работу (нарушение правил использования) средств защиты	0,6	средняя
Угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления	0,5	низкая
Сбой системы электроснабжения	0,7	средняя
Возможность сбора информации нарушителем об объектах атак	0,6	средняя
Угроза намеренного отключения средств защиты, внедрения вредоносных программ	0,7	средняя
Угроза физического доступа к каналам связи, коммутационному оборудованию	0,5	низкая
Угроза несанкционированного подключения к оконечному оборудованию	0,5	низкая

Оценка опасности угроз.

Оценка опасности УБ производится на основе опроса специалистов по защите информации и определяется показателем опасности, который имеет три значения:

- низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для инфраструктуры;
- средняя опасность – если реализация угрозы может привести к негативным последствиям для инфраструктуры;

- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для инфраструктуры.

Определение актуальности угроз в инфраструктуре.

В соответствии с принятыми правилами определения актуальности угроз безопасности в Таблице 5 определяются актуальные и неактуальные угрозы.

После определения перечня актуальных угроз выбираются мероприятия организационного, технического и физического характера по снижению опасности актуальных угроз и рисков. Перечень рекомендуемых мероприятий будет представлен ниже.

Таблица 5 – Определение актуальности угроз

Возможность реализации угрозы	Показатель опасности		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

В таблице 6 представлено итоговое определение актуальности угроз с учетом типов угроз безопасности и показателей опасности.

Таблица 6 – Актуальность угроз с учетом показателей опасности

Тип угроз безопасности	Показатель опасности	Возможность реализации
Угрозы утечки информации по каналам ПЭМИН	неактуальная	низкая
Нарушение работоспособности технических средств	актуальная	средняя
Вмешательство в работу (нарушение правил использования) средств	актуальная	средняя

Тип угроз безопасности	Показатель опасности	Возможность реализации
защиты		
Угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления	неактуальная	низкая
Сбой системы электроснабжения	актуальная	средняя
Возможность сбора информации нарушителем об объектах атак	актуальная	средняя
Угроза намеренного отключения средств защиты, внедрения вредоносных программ	актуальная	средняя
Угроза физического доступа к каналам связи, коммутационному оборудованию	неактуальная	низкая
Угроза несанкционированного подключения к оконечному оборудованию	неактуальная	низкая

Для снижения опасности реализации актуальных УБ необходимо принять следующие меры:

- проведение с администраторами регулярных семинаров по вопросам информационной безопасности;
- включение обязанностей в области защиты информации в должностные инструкции привилегированных пользователей;
- определение процедур увольнения сотрудников, занимавших должности привилегированных пользователей;

- организация обучения и инструктажей в области защиты информации;
- определения механизмов стимулирования и поощрения различного характера (в т.ч. финансового);
- организация, документальное оформление и внедрение принципов разграничения полномочий и двойного управления для решения задач, связанных с администрированием программных и технических средств, в том числе средств обеспечения ИБ;
- определение процедур реагирования на нарушения информационной безопасности;
- определение процедур контроля выполнения требований;
- установление ответственности за нарушения информационной безопасности.

2.3 Разработка плана DPR

План разрабатывается на основе анализа рисков, приводящих к возникновению ЧС, анализа воздействия ЧС на ключевые бизнес-процессы и имеет целью разработку решений на обеспечение безостановочности этих бизнес-процессов.

Для разработки плана DRP (далее – План) были выявлены ключевые бизнес-процессы при обработке и защиты информации, определены возможные угрозы техногенного характера, проанализированы и систематизированы зависимости ИТ-инфраструктуры от нештатных ситуаций. А также определение мер защиты от прерывания обработки информации и определение действий по восстановлению работоспособности элементов инфраструктуры и баз данных в случае воздействия деструктивных ситуаций на процесс обработки информации.

При определении техногенных и природно-техногенных рисков и угроз учитывались зависимости от внутренних процессов университета (как организационных, так и управленческих).

В структуру плана вошли следующие элементы:

- виды актуальных деструктивных событий;
- список групп реагирования по типам инцидентов, ролевого участия, временных рамок реагирования на инцидент;
- список ИТ-сервисов и зависимостей с соответствующими ресурсами;
- оценка угроз техногенного характера ключевым бизнес-процессам и информационным ресурсам;
- определение ролей и обязанностей сотрудников в чрезвычайных ситуациях;
- описание методов психофизического воздействия на сотрудников;
- описание порядка действий сотрудников;
- таблица возможных потерь в кратко и длинно срочной перспективе от остановки критичных бизнес-процессов, выхода из строя сетевого оборудования, потери информации на носителях, потери коммуникаций;
- техническое задание (проект) и регламент резервного копирования критически важной инфраструктуры и информации, включая функциональную схему резервирования ИТ-сервисов;
- регламент восстановления КВИ включающий в себя:
  - систематизацию инцидентов;
  - реагирование на инциденты;
  - определение взаимодействия при возникновении деструктивных ситуаций, схематичное распределение ответственности за оповещение групп реагирования с указанием типа оповещения и временных рамок;
  - порядок оповещения сотрудников, занятых в процедурах восстановления;
  - детальный план действий в режиме чрезвычайной ситуации;

- проведение тестовых испытаний;
- обучение сотрудников процедурам реагирования на инциденты и восстановления ИТ-инфраструктуры;
- порядок ознакомления сотрудников с планом;
- порядок внесения изменений для обновления плана.

Цель создания проекта Плана: обеспечение целостности информации и непрерывности критичных бизнес-процессов обработки информации.

В ходе реализации были исследованы:

- расположение ключевых узлов инфраструктуры сети;
- частота событий техногенного характера;
- совокупность вероятности наступления событий и возможного ущерба;
- расположение всех видов коммуникаций относительно сетевого оборудования и каналов связи;
- расположение помещений, в которых обрабатывается КВИ;
- схема пожароохранной сигнализации;
- расположение и оборудование контролируемых зон;
- физическая охрана объектов КВИ;
- состав групп реагирования и ответственных лиц на кризисные и аварийные ситуации;
- профессиональная компетентность участников групп реагирования;
- существующий порядок оповещения соответствующих служб при авариях;
- состав и наличие резервных схем электропитания и водоснабжения;
- состав КВИ;
- пропускная способность каналов связи;
- возможность резервирования каналов связи;
- актуальные угрозы при наступлении событий чрезвычайного и аварийного характера;

- приемлемость рисков исходя из угроз;
- максимальное время простоя ключевых бизнес-процессов;
- площадки резервного копирования;
- состав резервируемой информации;
- текущие процедуры резервного копирования;
- процедуры восстановления данных и временные рамки;
- возможность зеркалирования баз данных и оперативного переключения источников данных;
- существующие средства защиты информации.

2.4 Определение методов и разработка программы научных исследований

Методы научных исследований зависят от типа исследования соотносительно к цели исследования. Так же согласно определяемой цели исследования могут быть классифицированы или как прикладные, или как фундаментальные.

Прикладное исследование предназначено находить решение для непосредственной и определенной проблемы (проблем). Соответственно, результаты исследований ценны на практических уровнях и могут быть применены на практике.

Процесс от теоретических предпосылок к результату не может быть линейным, скорее круговым или спиральным, т.к. всякий результат тестирования гипотезы может быть лучшим предыдущего, что и обуславливает саморазвитие науки (рисунок 7).

Теория построения и теоретическое тестирование особенно сложны в создании моделей безопасности, учитывая неточный характер теоретических концепций, специфический инструментарий для их измерения и наличие многих неучтенных факторов, которые также могут влиять на конечные выводы и результат исследования в целом.

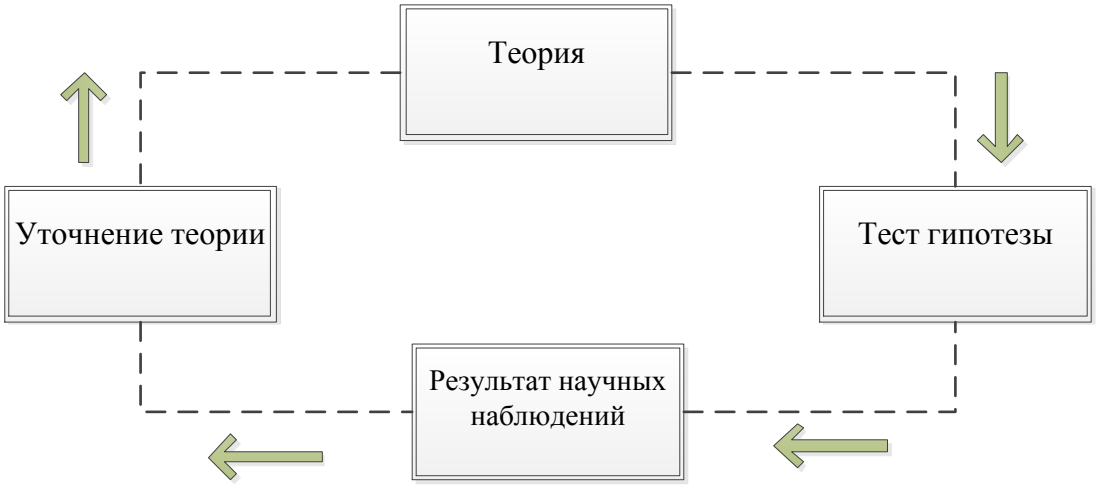

Рисунок 7 – Процесс исследования

В нашем случае:

Цель исследования: Анализ рисков возникновения внештатных ситуации и их деструктивного воздействия на защищаемую информацию и инфраструктуру локальной вычислительной сети.

Объект исследования: Тольяттинский государственный университет.

Предмет исследования**:** Инфраструктура сети, оборудования, информационных активов, персонал.

Общенаучный метод работы основан на предположении, что организация защиты информации в образовательном учреждении будет производиться более эффективно и качественно на основе оценки и анализа существующих рисков, если:

- рассмотрены подходы и методологические основания к исследованию информационной безопасности при возникновении ЧС;
- будут проанализированы риски возникновения ЧС и определены критерии их приемлемости;
- будет смоделирован алгоритм действий сотрудников при возникновении ЧС на основе имитационной модели угроз безопасности;

- будет проведена оценка эффективности применяемых средств защиты от воздействия деструктивных факторов;
- будет проведена работа по предупреждению и предотвращению чрезвычайных ситуаций на территории университета;
- будет проведено определение зависимости рисков от средств, вложенных в мероприятия информационной безопасности.

Помимо выбранного для исследований общенаучного метода, основанного на эмпирическом уровне, будут проведены лабораторные эксперименты по измерению параметров работы оборудования, математические зависимости, тематические исследования влияния техногенных факторов на инфраструктуру сети, психофизического воздействия чрезвычайных ситуаций на работу персонала.

В соответствии с целью исследования проект решения будет сгруппирован по трем типам: исследовательский, описательный и пояснительный.

Исследовательские исследования описывают возможные масштабы конкретных деструктивных ситуаций, возникающие проблемы или поведенческие реакции и проверяет осуществимость исследования этих ситуаций, частоту возникновения, актуальность для разрабатываемой модели угроз, и служить в качестве исходных данных для выполнения целевой задачи.

Описательные исследования направлены на тщательные наблюдения и подробное документирование интересующего события или явления. Эти наблюдения основываются на научном методе (т.е. должны быть реплицируемыми, точными и т.д.) и, следовательно, более надежными, чем случайные наблюдения и соответствующие выводы, основанные на анализе недостаточных или неполных данных.

Пояснительные исследования приводят объяснения наблюдаемых явлений, поведенческих реакций. Хотя описательные исследования исследуют, что, где и когда произошло, пояснительное исследование ищет

ответы на вопрос о том, почему и как, определяя причинные факторы и результаты целевого явления или события.

Исходя из вышесказанного, получаем более полный цикл исследования проблемы (рисунок 8).

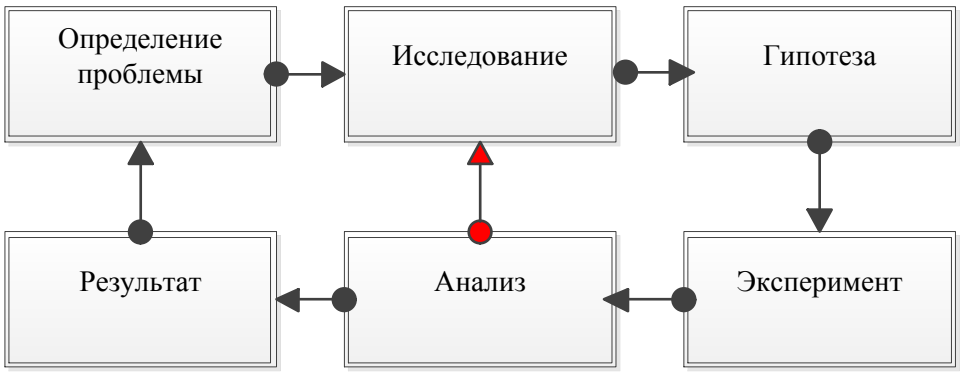

Рисунок 8 – Цикл исследования проблемы

Для исследования проблемы будет применен системный подход. Системный подход условно можно разбить на следующие этапы:

- определение объекта исследования, задание параметров для изучения объекта и управления им;
- первичная структуризация и определение границ изучаемой системы;
- разработка математической модели определяемой системы;
- исследование разработанной математической модели, проведение анализа результатов построенной модели;
- выбор способа управления системой.

Выбор способа управления системой позволяет перевести ее в желаемое состояние для решения проблемы.

Вывод: Разработанная методика оценки рисков, внедрения плана восстановления позволяют реализовывать мероприятия по обеспечению безопасности в соответствии с актуальной моделью угроз.

3 Проведение теоретических и экспериментальных исследований

3.1 Определение методики исследования

Любая теория представляет собой набор взаимосвязанных понятий, определений и предложений, которые объясняют или предсказывают события, или ситуации (а также явления, тенденции, процессы и т.д.), основываясь на различных предположениях и их отношениях между собой.

Цель теоретических методов исследований – получение новых знаний о предмете исследования, а также эмпирическое понимание, исследование и объяснение существующей реальности.

Для решения задачи исследования защищенности сетевой инфраструктуры и информации будут выбраны теоретические методы логического анализа и моделирования.

Для формулировки гипотезы актуальности угроз безопасности информации от событий техногенного характера потребуется анализ существующих решений в отрасли в сравнении с принятыми на сегодняшний день в образовательном учреждении в зависимости от актуальных угроз безопасности.

Гипотеза должна быть:

- концептуально понятной;
- конкретной;
- иметь возможность тестирования;
- должна быть связана с имеющимися методами исследований;
- логически последовательной;
- объективной;
- как можно более простой.

Конечная цель проведенных исследований – создание систем предупреждения аварийных ситуаций, разработка организационных мер с

учетом выводов исследований, разработка плана восстановления, мер по исключению НСД в ИС в условиях отказов ее функционирования, систем жизнеобеспечения при стихийных бедствиях, а также прогнозирование связанных инцидентов безопасности.

3.2 Методология теоретического исследования

Методы исследований – это набор методов, используемых во всех науках. Методы включают такие процедуры, как формирование концепций и гипотез, проведение наблюдений и измерений, проведение экспериментов, построение моделей и теорий, предоставление объяснений и прогнозирование.

Цель методологии – описать и проанализировать методы, сделать обобщения относительно успеха методов, используемых для предложения новых методов или подходов. Методология заключается в том, чтобы помочь нам понять не только результаты научного исследования, но и процесс [12].

Обзор литературных источников показывает, что организация мероприятий по защите информации в чрезвычайных ситуациях осуществляется безотносительно к отрасли, к особенностям инфраструктуры, региона, подготовки обслуживающего персонала. Соответственно разными являются модели угроз безопасности информации, создаваемые на оценке рисков, в свою очередь вытекающие из упомянутых выше параметров.

Итак, на данном этапе определены теории и модели, которые выбраны для использования для ответа на исследовательские вопросы.

Самым важным шагом является правильный выбор и формулировка проблем исследования. Термин «проблема» означает определить гипотетически вопрос, подлежащий рассмотрению. Сформулировать проблему означает преобразовать выбранную задачу исследования в научно обоснованный вопрос.

В первую очередь анализируются риски возникновения ЧС и определяются критерии их приемлемости.

При анализе явлений и процессов рассматривается большой кейс признаков. Для этого применяется способ ранжирования, с помощью которого исключается второстепенное, не существенное для рассматриваемой проблемы.

Под чрезвычайной ситуацией понимаются множество явлений событийного характера, приводящие в результате к нарушению штатного функционирования СЗИ через проявление ряда уязвимостей средств защиты и программного обеспечения инфраструктуры, при этом характеризующиеся слабой степенью прогнозирования.

Базируясь на типах событий техногенного характера, включая возможные аварийные ситуации, прогнозирования их возникновения для региона и образовательного учреждения можно выделить следующие:

- наводнения (затопление коммуникаций);
- разрушения, вызванные ураганами;
- поражение инфраструктуры от грозовых разрядов;
- пожары;
- отказ систем жизнеобеспечения;
- несанкционированный доступ к информации с целью информационного воздействия или ее искажения для затруднения управленческих решений;
- теракты на объектах инфраструктуры.

Далее следует теоретический анализ (оценка) опасных и вредных факторов, генерируемых элементами среды обитания (технологические процессы, инфраструктура, природные и социальные явления) на основе которого исследуются проблемы:

- компетенций персонала, привлекаемого к мероприятиям по организации защиты информации и эксплуатации средств защиты;
- контроля и мониторинга состояния инфраструктуры и средств защиты;

- моделирования и прогнозирования развития чрезвычайных ситуаций и их возможного влияния на работоспособность информационных каналов и целостности, и доступности информации;
- расчет рисков как вероятность возникновения негативных факторов, влияющих на функциональность объектов инфраструктуры;
- социопсихологических аспектов восприятия и оценки приемлемости риска;
- пропускной способности каналов связи в зависимости от факторов окружающей среды;
- производительности серверов и сохранности информации в зависимости от температуры и влажности серверных помещений, организации электроснабжения;
- рационального использования средств защиты информации от негативного воздействия техногенных источников и стихийных явлений.

И как конечный результат – разработка плана по ликвидации последствий чрезвычайных и аварийных ситуаций в области защиты информации и сетевой инфраструктуры образовательного учреждения.

3.3 Методология экспериментальных исследований

В целом экспериментальный метод исследований является систематическим и научным подходом к исследованию проблем, в которых исследователь манипулирует одной или несколькими переменными, а также контролирует и измеряет любые изменения в других переменных.

В нашем случае в качестве входных значений переменных для эксперимента будут использоваться изменяющиеся факторы окружающей среды, событий чрезвычайных и аварийных ситуаций, параметры систем

жизнеобеспечения и контроль изменений в инфраструктуре сети, каналах связи, системах защиты информации и целостности информации.

Для исследования некоторых проблем из вышеозначенного списка, связанных с инструментальными исследованиями, формулируются гипотезы.

Методология эксперимента выбирается исходя из ряда факторов. Важными факторами при выборе методологии являются выполнимость, время, проблемы с измерением и прогнозируемый результат.

Одним из разделов исследований по обозначенной тематике выбрано исследование производительности серверного оборудования в зависимости от внешних факторов, вызываемых аварийными ситуациями или нештатной работой систем электроснабжения и вентиляции.

Цель эксперимента: изучить изменение характеристик производительности объекта от изменяющихся внешних факторов, проанализировать последствия от возникновения чрезвычайных ситуаций.

План-программа эксперимента:

- описать существующее решение схемы электроснабжения;
- описать существующее решение схемы кондиционирования и вентиляции;
- расчет рисков как вероятность возникновения нештатных ситуаций с электроснабжением и пожаром на объекте;
- сформулировать гипотезу эксперимента;
- определить способы измерения производительности объектов системы от изменяющихся характеристик окружающей среды;
- провести эксперимент;
- представить результаты в виде графиков зависимостей поведения объектов от входных параметров;
- проанализировать полученные результаты;
- сформулировать выводы по подтверждению или опровержению выдвинутых гипотез и определить их практическое применение.

3.4 Изучение и освоение теоретических моделей и физических характеристик оборудования систем жизнеобеспечения серверной комнаты и влияние их на производительность серверного оборудования при изменяющихся параметрах, вызванных аварийными и нештатными ситуациями

3.4.1 Этапы проведения исследований

Этап 1. Описание решения схемы электроснабжения, кондиционирования и вентиляции серверного помещения.

В результате проведения экспериментов нужно получить значение идеальной температуры в серверной комнате, которая может обеспечить оптимальную эффективность работы всех сетевых компонентов.

Как и для всех механических компонентов, агрессивной средой для электронных компонентов являются тепло и влажность. Каждая из частей компьютерного оборудования, которая включает процессор, материнскую плату, и остальные комплектующие имеют диапазон температур, в которых они работают с оптимальной эффективностью.

Резкое изменение этого оптимального температурного диапазона может привести к поломке, серьезно влияя на его работу.

Рассмотрим факторы, которые определяют идеальную температуру для серверных комнат.

Каждый электронный компонент, который является частью сервера и связанного с ним оборудования, генерирует определенное количество тепла благодаря его функционированию. В идеале, для определения правильной комнатной температуры необходимо изучить оптимальный диапазон рабочих температур для каждого компонента и соответственно установить уровни температуры и влажности в серверной комнате.

Таким образом, одним из главных факторов является тепловая мощность каждого из его компонентов компьютерного оборудования и их оптимальный диапазон производительности. Конечно, число компьютерных систем,

коммутаторов и других подобных сетевых компонентов также влияет на выбор температурного диапазона.

Самое главное, размер комнаты, поскольку он будет определять мощность системы кондиционирования, которая понадобится для поддержания идеальной температуры. В нашем случае размер составляет 838 мм * 535 мм.

Установленная температура системы кондиционирования воздуха и уровней влажности должна быть точно откалибрована, чтобы тепло, выделяемое компонентами, эффективно отводилось путем циркуляции воздуха. Уровни температуры и влажности не могут быть слишком низкими или высокими.

Система электропитания разнесена по трем фазам с автоматическим аварийным переключением на резервную схему электропитания.

Схема серверной комнаты приведена на рисунке 9.

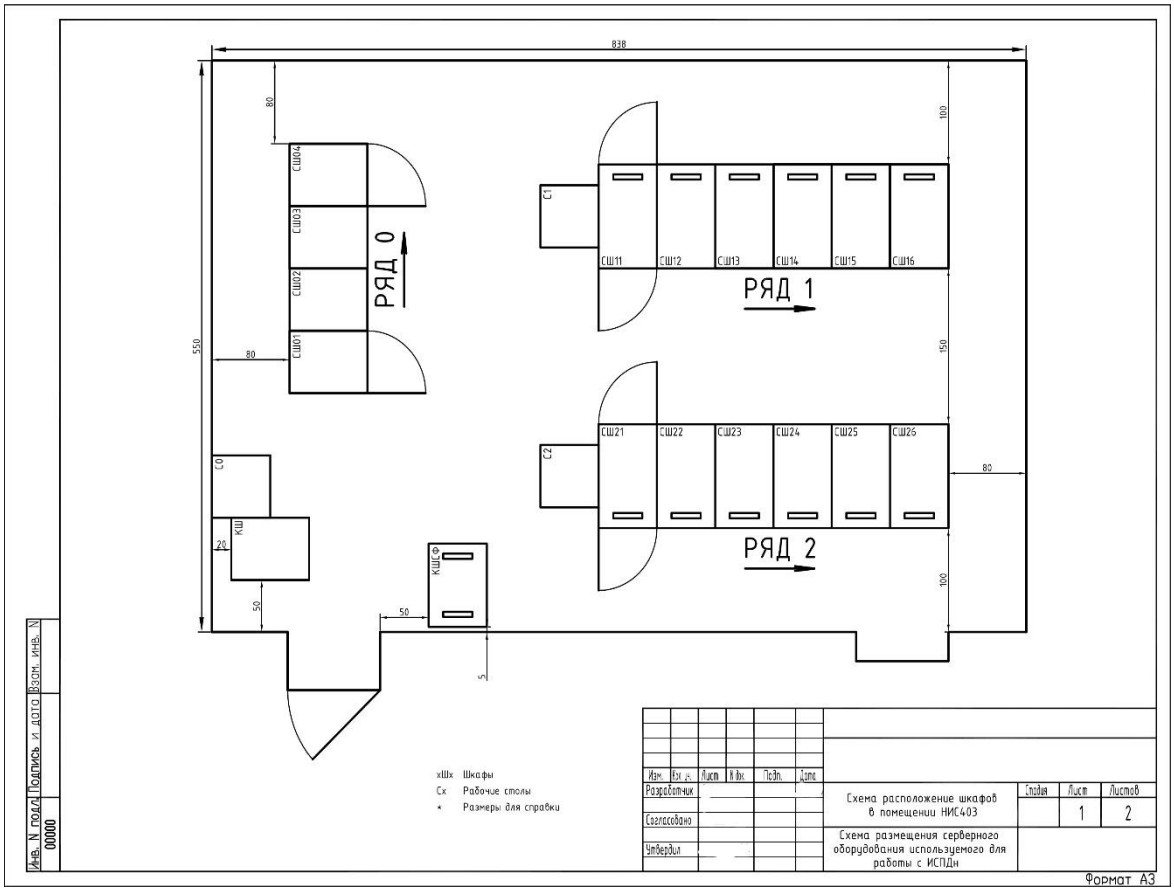

Рисунок 9 – Схема серверной комнаты

Этап 2. Расчет оптимальных параметров функционирования серверного оборудования.

Исходные данные для расчета:

- длина серверного помещения – 8,38 м;
- ширина серверного помещения – 5,50 м;
- высота серверного помещения – 2,80 м;
- площадь серверного помещения S = 46,09 м^2;
- объем серверного помещения V = 129 м^3;
- серверных стоек (шт.) – 17
- серверов (шт.) – 87
- коммутаторов (шт.) – 8

Для расчета тепловыделения оборудования в BTU/h умножаем значение максимальной потребляемой мощности на 3,412: T = P * 3,412.

Для расчета количества холодопроизводительности используем формулу:

$$Ph = Ts + Tn + To, \quad (3.1)$$

где Ph – холодопроизводительность кондиционера, измеряется в кВт;

Ts – тепловыделения всего оборудования;

Tn – тепловыделения от находящихся в помещении людей;

To – тепло, поступающее в помещение от окружающей среды.

Суммарное тепловыделение оборудования представлено в таблице 7.

Таблица 7 – Суммарное тепловыделение оборудования

Наименование оборудования	Максимальная потребляемая мощность, Вт (на единицу)	Тепловыделение (на единицу), BTU/h	Тепловыделение (всего), BTU/h
Сервер	380	1296,94	112833,78
Коммутатор	40	136,52	1092,16
ИТОГО			113925,94

Тепловыделения Th = 0, т.к. помещение не обитаемо.

Для расчета тепла, поступающего от окружающей среды, используем формулу:

$$Тм = V * q / 1000, (3.2)$$

где V – это объем помещения в $м^3$;

q – это коэффициент, зависящий от теплопроводности внешних стен, в расчетах принимается от 30 ватт/$м^3$

q = 387, Тм = 4,9

Ph = 113925,94 + 0 + 4,9 = 113930,84 BTU/h или 33,39 кВт

Рекомендация по температуре серверного помещения составляет от 20 C до 21 C . Хотя в отдельных случаях температура может изменяться в зависимости от тепловой мощности оборудования, не рекомендуется устанавливать ее ниже 10 °C и выше 28 C .

Влажность помещения (относительная) должна поддерживаться от 40 % до 50 %.

При дальнейших расчетах и исследовании ориентируемся на приведенные параметры.

Этап 3. Исследование производительности объекта от изменяющихся внешних факторов.

Гипотеза – производительность объекта падает при критическом повышении температуры окружающего воздуха при аварийном выходе из строя системы кондиционирования.

Начальная температура в помещении 19 °C.

Температура процессора 27 C, при минимальной нагрузке и скорости вентилятора 1034 RPM (рисунок 10), изменение температуры в динамике при незначительном повышении нагрузки на рисунке 10.

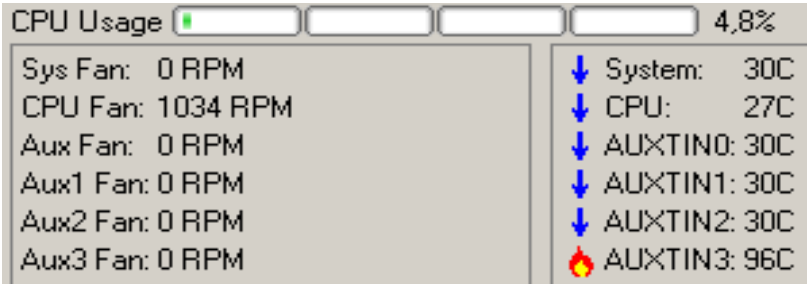

Рисунок 10 – Температура процессора при минимальных значениях

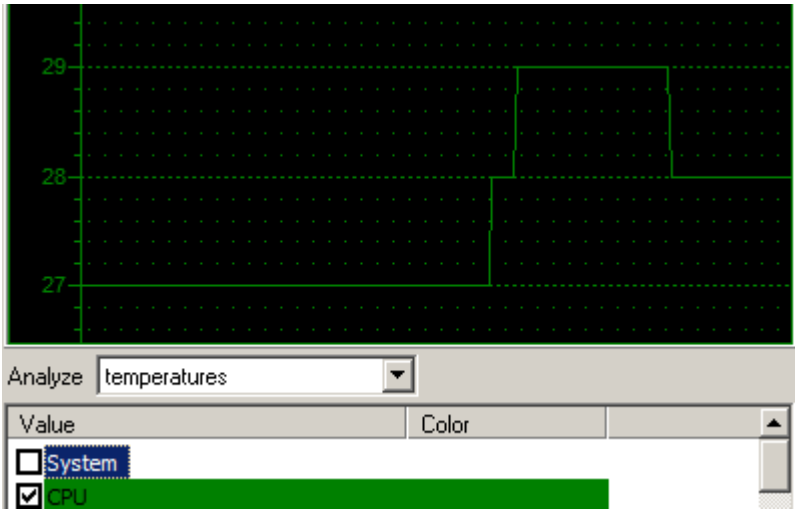

Рисунок 11 – Изменение температуры процессора в динамике

При искусственном отключении системы кондиционирования были произведены шаговые измерения нарастающей температуры в помещении и соответственно повышение температуры процессора в течение временного интервала (мин.). График представлен на рисунке 12.

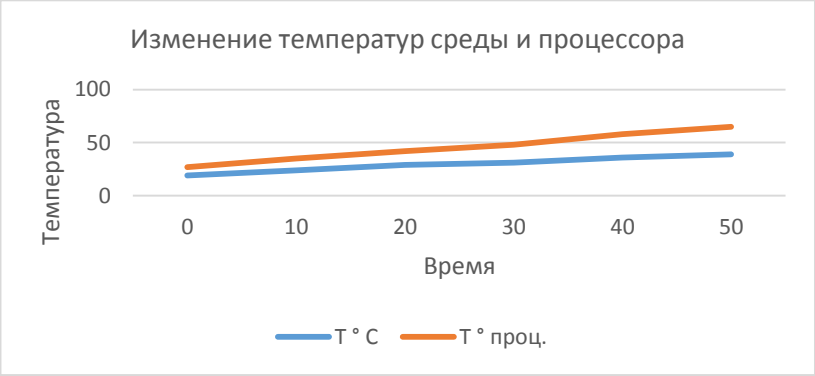

Рисунок 12 – График изменения температуры процессора и среды

Температура корпуса процессора при почти неизменной нагрузке и одной и той же скорости вентилятора будет находиться практически в линейной зависимости от температуры воздуха в корпусе, т.е. окружающей среды.

При повышении нагрузки процессора до 100 % наблюдаем значительное повышение температуры корпуса процессора до 57 °С (рисунок 13).

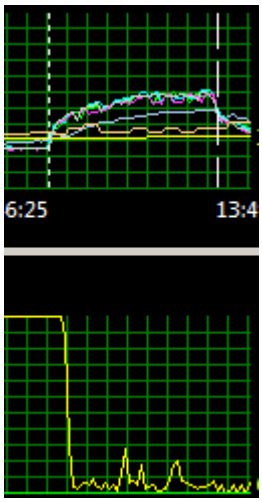

Рисунок 13 – Зависимость температуры процессора от нагрузки

Тактовая частота при максимальной нагрузке достигает 3020 МГц (рисунок 14).

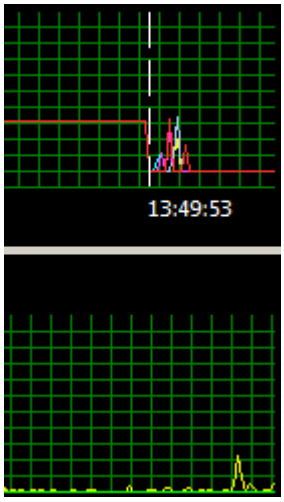

Рисунок 14 – Тактовая частота при максимальной нагрузке

На диаграмме, приведенной на рисунке 15, видно, что производительность процессора при нагреве до 75 °С плавно снизилась в 1,9 раз. То есть, количество холостых пакетов, выполняемых процессором, даже не составляет и половины от числа эффективных пакетов. После того, как процессор начал резко охлаждаться (включено охлаждение помещения), производительность так же резко вернулась на исходное значение.

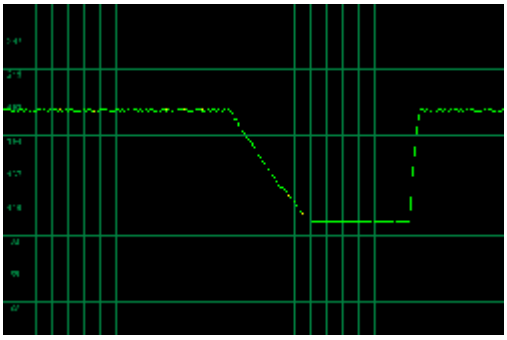

Рисунок 15 – Снижение производительности процессора

Этап 4. Формулировка выводов по результатам эксперимента.

При аварийном отключении систем кондиционирования через 40 минут при нагреве процессора до 75 С начинаются отклонения в режиме работы серверов (потеря пакетов трафика (Throttling)), при дальнейшем повышении температуры при загрузке процессора близкой к максимальной и соответственно суммарной температурой более 90 С полное отключение системы.

Этап 5. Практическое применение результатов исследования.

Исходя из расчетов хладоотведения, в помещении серверной должны быть установлены кондиционеры суммарной мощностью 33 кВт. При этом для исключения одновременного отключения при потере электроснабжения подключать следует на разные цепи питания.

Для оперативного мониторинга и управления режимами работы кондиционеров применяется специализированное WEB-приложение. На

рисунке 16 показан WEB интерфейс управления кондиционерами серверного помещения университета.

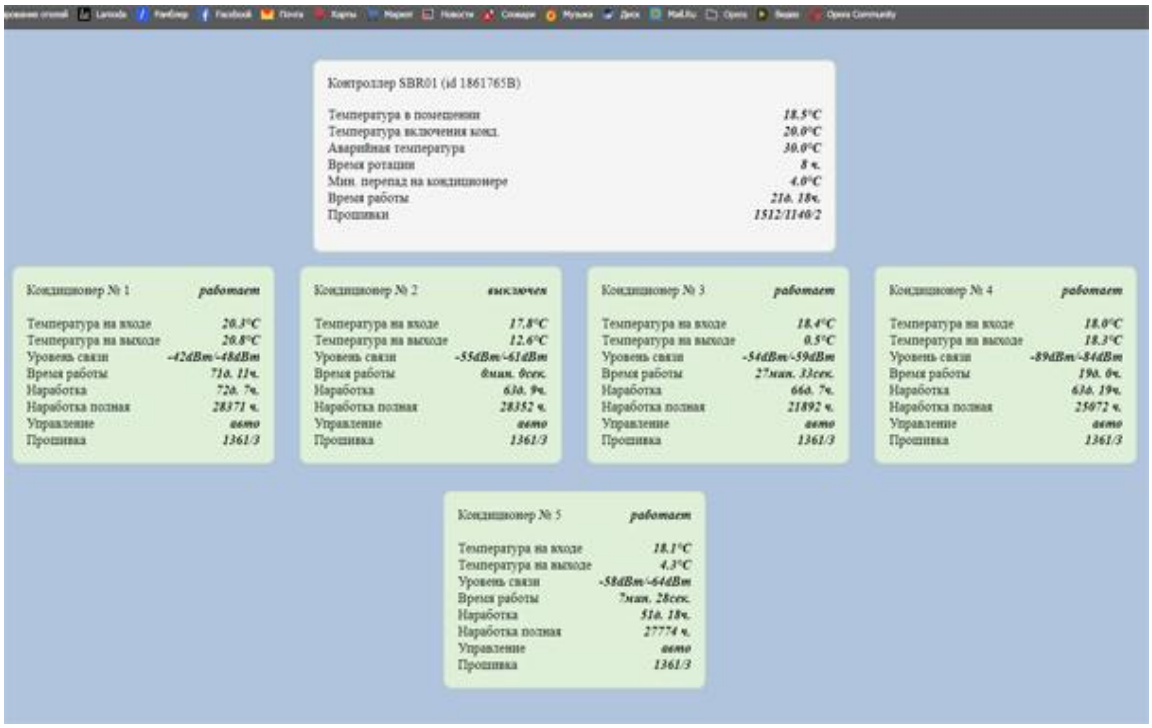

Рисунок 16 – WEB-интерфейс управления кондиционерами

3.4.2 Объект испытаний

Объектом исследований является процессор INTEL XEON E5-2630 v.2, характеристики которого приведены в таблице 8.

Таблица 8 – Характеристики процессора

Наименование характеристики	Значение
Тактовая частота	2,60 GHz
Максимальная частота (турбо)	3,10 GHz
Частота системной шины	7,2 GT/s QPI
TDP (мощность для расчета теплоотведения)	80W
Память	128 ГБ (DDR3 800/1066/1333/1600)
TCASE (максимальная температура на корпусе процессора)	71 °C

3.4.3 Оборудование, используемое при измерениях и обработке результатов

Применяемый исследовательский аппаратно-программный комплекс, включает в себя:

- программно-аппаратный комплекс управления системой кондиционирования;
- систему резервного электроснабжения;
- силовые и телекоммуникационные линии;
- программное обеспечение измерения производительности процессора;
- электронный термометр с дистанционным датчиком;
- гигрометр;
- ПО для снятия характеристик процессора.

3.4.4 Условия проведения исследований

Исследования проводились при изменяющихся температуре окружающего воздуха и относительной влажности посредствам управления системой кондиционирования воздуха в серверном помещении, а, так же нагрузочным изменением режима работы охлаждения процессора.

3.4.5 Результаты исследований

Полученные результаты исследований представлены на рисунках 10-15 и в таблице 7.

3.5 Анализ результатов исследований, формулирование выводов и рекомендаций

Выбор тематики исследования обусловлен актуальностью риска возникновения аварийных ситуаций, вызванных отключением системы электроснабжения, пожара в серверном помещении.

Критическое повышение температуры заставляет кабели смягчаться, расширяться, провисать и т.д. Это увеличивает задержку прохождения пакетов информации и может приводить к потере пакетов (и, следовательно, влечет за собой повторные передачи, уменьшая эффективную пропускную способность). Это относится как к оптоволокну, так и к витой паре, но не к подземному кабелю (который термически изолирован).

Тепло также приводит к сбою активных устройств, если они не охлаждаются принудительно, или, когда охлаждение является недостаточным.

Поэтому идеальные уровни температуры и влажности определяются всеми производителями серверного оборудования. Их значения должны поддерживаться в определенном диапазоне.

В результате теоретико-экспериментального анализа исследований установлено совпадение рабочей гипотезы, теоретических предпосылок с результатами опыта по измерению режимов работы процессора при нарастающей температуре окружающего воздуха, вызванного аварийной ситуацией.

Пересмотра или корректировки рабочей гипотезы не потребовалось, выводы, полученные в результате исследования, имеют практическое значение.

3.5.1 Анализ полученных результатов исследований

Результаты проведенных исследований свидетельствуют о необходимости учитывать особенности организации хладоотведения из серверного помещения, учитывая размеры, объем, расположение комнаты, характер, мощность и количество серверного оборудования, температурные режимы штатной работы инфраструктуры и особенности работы при наступлении критических ситуаций. При разработке Плана восстановительных работ необходимо предусмотреть мероприятия по восстановлению системы хладоотведения во временных рамках, не

превышающих 50 минут. В это время необходимо учитывать оповещение и время прибытия группы специалистов.

3.5.2 Выводы по результатам исследований

Анализ полученных результатов исследований позволяет сделать вывод о спаде производительности систем при выходе из строя части кондиционеров, а также при критических значениях температуры окружающего воздуха полному их отключению вследствие аварий электроснабжения систем кондиционирования при несвоевременном обнаружении данного факта или нарушений систем управления. Также следует сделать вывод об эффективности внедрения систем аварийного электроснабжения серверного помещения и дистанционного мониторинга и управления системой кондиционирования воздуха.

3.5.3 Рекомендации

Следует рекомендовать применение приточно-вытяжной вентиляции, ввиду тепловой нагрузки более 400 Вт/м^2 установить способ вентиляции снизу-вверх (рисунок 17), 4-5 кондиционеров (с учетом резерва) суммарной мощностью 34-35 Квт, Web-интерфейса мониторинга работы системы кондиционирования, автоматическое SMS-информирование ответственного лица об аварийных ситуациях в серверной, организацию автоматического (программного) подключения/отключения кондиционеров для поддержания оптимальной температуры и влажности, автоматическое переключение цепей электроснабжения на резервные линии при авариях, устранение аварийной ситуации за временной промежуток не более 50 минут с целью обеспечения максимальной производительности и непрерывности работы серверного оборудования и, как следствие, обеспечение целостности и доступности обрабатываемой на серверах информации.

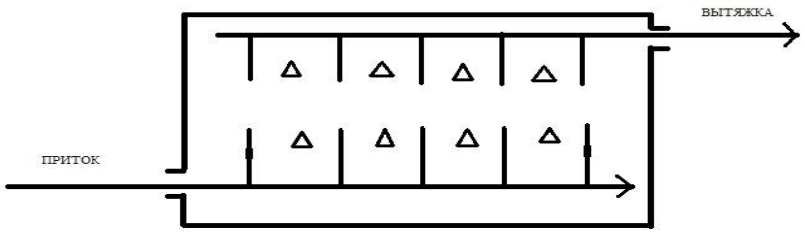

Рисунок 17 – Схема приточно-вытяжной вентиляции

Вывод: Приведенные данные позволяют получить повышение надежности оборудования, говорят об эффективности внедрения систем аварийного электроснабжения серверного помещения и дистанционного мониторинга и управления системой кондиционирования воздуха, позволяют достичь снижения воздействия антропогенных факторов.

ЗАКЛЮЧЕНИЕ

Результатом выполнения исследовательских работ является получение практических навыков описания алгоритма проведения теоретических и экспериментальных исследований, проведению исследования выбранного объекта, анализу результатов исследований и формулировке выводы и рекомендации к практическому применению полученных результатов.

В рамках данной работы поставленные задачи для достижения цели решены в полном объеме.

Было определено, что безопасность информационной инфраструктуры образовательного учреждения является обязательным условием и одним из критериев эффективности деятельности образовательного учреждения и обеспечения качества образования. Проанализированы существующие методики действий при возникновении внештатных ситуаций, при этом отмечено отсутствие отраслевых методик действий. За рубежом широко применяется план DPR – восстановление инфраструктуры после деструктивных событий. У нас в стране подобный план только начал появляться на рынке услуг инфраструктуры ИБ. Все это обусловило выполнение основной цели работы – разработку алгоритма организации системы защиты для обеспечения информационной безопасности на объектах инфраструктуры при возникновении чрезвычайных и аварийных ситуаций.

Были определены риски безопасности, на основе которых разработана модель угроз, определены актуальность угроз и сформулированы методы минимизации рисков применительно к существующей инфраструктуре и прогнозированию ситуаций.

На основе актуальности угроз схематически разработан план восстановления инфраструктуры, разработан и приведен в приложении А план действий ответственных лиц во внештатных ситуациях.

Произведен математический расчет рисков несанкционированного доступа к информации в условиях возможности деструктивных событий.

Сформулирована методика организации защиты информации в чрезвычайных и аварийных ситуациях как непрерывный управленческий процесс.

Определена методология теоретического исследования целевой проблемы с конечной целью создания систем предупреждения аварийных ситуаций, разработки организационных мер с учетом выводов исследований, мер по исключению НСД в ИС в условиях отказов ее функционирования, систем жизнеобеспечения при стихийных бедствиях.

Произведен теоретический анализ (оценка) опасных и вредных факторов, генерируемых элементами среды обитания (технологических процессов, инфраструктуры, природных и социальных явлений).

Был проведен эксперимент с целью подтвердить сформулированную гипотезу, изучить изменение характеристик производительности объекта от изменяющихся внешних факторов, проанализировать последствия от возникновения чрезвычайных ситуаций.

В ходе эксперимента проведено изучение и освоение теоретических моделей и физических характеристик оборудования систем жизнеобеспечения серверной комнаты и влияние их на производительность серверного оборудования при изменяющихся параметрах, вызванных аварийными и нештатными ситуациями.

По результатам исследований сформулированы выводы, на основании которых выработаны рекомендации с целью обеспечения максимальной производительности и непрерывности работы серверного оборудования и, как следствие, обеспечение целостности и доступности обрабатываемой на серверах информации.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1 Власов, И.А. Моделирование угроз безопасности информации в автоматизированных системах управления (асу) техносферной безопасностью / И.А. Власов; Научные вести - 2018, - №3 УДК 338.341.018 - С. 23-29. [Электронный ресурс] URL: http://www.nvesti.ru/wp-content/uploads/2018/10/журнал_Научные_вести_3.pdf (дата обращения: 29.03.2019).

2 Дубовик, О.Л. «Экологическое право» Учеб. - методическое пособие / Дубовик О.Л. - М. : Проспект, ТК Велби, 2007. - 688 с.

3 COBIT® 5 ISBN 978-1-60420-290-8 © 2012 ISACA. Руководство по использованию. [Электронный ресурс]. URL: www.isaca.org/COBITuse (дата обращения: 15.03.2019).

4 Definitive 7 Point Disaster Recovery Planning Checklist [Электронный ресурс]. URL: https://phoenixnap.com/blog/disaster-recovery-plan-checklist (дата обращения: 04.04.2019).

5 Статистика от ISASA [Электронный ресурс]. URL: http://www.isaca.org/cyber/Documents/State-of (дата обращения: 01.04.2019).

6 Мельников, В.П., Информационная безопасность и защита информации / Клейменов С.А., Петраков А.М; 3-е изд., стер. - М. : Наука, 2008. - 336 с.

7 ISO/IEC 31010, Risk management — Risk assessment techniques. Checklist [Электронный ресурс]. URL: https://www.dvbi.ru/risk-management/library/Token/ViewInfo/ItemId/8/ISO-31010-2009-Risk-Management-Risk-Assessment-Techniques-eng-rus (дата обращения: 28.03.2019).

8 Технология информационного обеспечения бизнес-процессов в экстремальных ситуациях. Открытое образование – 2010, - №4 УДК

004.853 ББК 20 [Электронный ресурс]. URL: https://doi.org/10.21686/1818-4243-2018-4 (дата обращения: 29.03.2019).

9 ГОСТ Р ИСО/МЭК 17799- 2005 Практические правила управления информационной безопасностью [Электронный ресурс]. URL: http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005 (дата обращения: 19.03.2019)

10 ISO/IEC 27002 Информационные технологии. Свод правил по управлению защитой информации. [Электронный ресурс]. URL: https://files.stroyinf.ru/Data2/1/4293777/4293777199.pdf (дата обращения: 03.04.2019).

11 Горина, Л.Н Производственная практика «научно-исследовательская работа» по направлению подготовки магистров «Техносферная безопасность», Учеб. - методическое пособие. – Тольятти: Изд-во ТГУ, 2016. – 33 с.

12 Гатчин, Ю.А. Технология информационного обеспечения бизнес-процессов в экстремальных ситуациях / Ю.А. Гатчин, С.А. Арустамов, В.В. Сухостат, - М. : Открытое образование, 2010. – № 4. – С. 10–20.

13 Гришина, Н.В. Организация комплексной системы защиты информации / Н.В. Гришина; - М. : «Гелиос АРВ», 2007. 256 с.

14 Краснов, А.В., Горина, Л.Н. Научно-исследовательская работа. По направлению подготовки 20.04.01 «Техносферная безопасность». - Тольятти: изд-во ТГУ, 2016. – 164с.

15 Abraham Kaplan The Conduct of Inquiry: Methodology for Behavioral Science / A. Kaplan; -M. : San Francisco.Chandler, 1964, – 262 с .

16 ГОСТ 22261-94. Средства измерений электронных и магнитных величин. Общие технические условия. [Электронный ресурс]. URL: http://docs.cntd.ru/document/gost-22261-94 (дата обращения: 19.03.2019)

17 ИСО/МЭК ТО 13335-3-2007 Методы и средства обеспечения безопасности [Электронный ресурс]. URL: http://internet-law.ru/gosts/gost/5475/ (дата обращения: 17.03.2019).

18 ГОСТ 8.558-93 ГСИ. Государственная поверочная схема для средств измерений температуры [Электронный ресурс]. URL: https://www.internet-law.ru/gosts/gost/38387/ (дата обращения: 27.03.2019).

19 ГОСТ 12.0.002-80 (1999) ССБТ. Термины и определения [Электронный ресурс]. URL: http://internet-law.ru/gosts/gost/61000/ (дата обращения: 17.03.2019).

20 Стандарт COBIT 5: Бизнес-модель по руководству и управлению ИТ на предприятии [Электронный ресурс]. URL: http://www.wikiitil.ru/books/Cobit-5_frm_rus_0813.pdf (дата обращения: 24.03.2019).

21 СанПиН 2.2.4.548-96 Санитарные нормы микроклимата производственных помещений [Электронный ресурс]. URL: http://www.tehbez.ru/docum/documshow_documid_333.html (дата обращения 03.04.2019).

22 Федеральный закон от 21.12.1994 N 69- ФЗ «О пожарной безопасности» (последняя редакция) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_5438/ (дата обращения: 02.04.2019).

23 Федеральный закон от 28.12.2010 N 390-ФЗ "О безопасности" [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_108546/ (дата обращения: 12.04.2019).

24 Федеральный закон от 06.12.2007 №99-ФЗ «О лицензировании отдельных видов деятельности» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_113658/ (дата обращения: 05.04.2019).

25 Приказ ФСТЭК от 18.02.2013 г. №21 « Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в

информационных системах персональных данных». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_146520/ (дата обращения 13.04.2019).

26 Козак, Н.Н. Правовые основы и практическое обеспечение комплексной безопасности в организациях / Н.Н. Козак; Учебное пособие. – М. : Издательские решения, 2016 – 246 с.

27 Игнатьев, В.А. Информационная безопасность современного коммерческого предприятия / В.А. Игнатьев; Монография. Старый Оскол, М. : ООО «ТНТ», 2005. – 448 с.

28 Емельянников, М.В. Безопасность цифровой личности в государственных системах: резервное копирование и восстановление данных / М.В. Емельянников; М. : «Veeam», 2015, –215 с.

29 Таненбаум, Э. Т18 Компьютерные сети/ Э. Таненбаум, Д. Уэзеролл; М. : СПб.Питер, 2012. — 960 с.

30 Бадалова, А.Г. Управление рисками деятельности предприятия / А.Г. Бадалова; Учебное пособие. М. : Вузовская книга, 2016. — 234 с.

Приложение А

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Инструкция
действий должностных лиц по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций

Тольятти 2019

Содержание

1. Область применения

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационной инфраструктуры в ФГБОУ ВО «Тольяттинский государственный университет» (далее – Университет), меры и средства поддержания непрерывности работы и восстановления работоспособности инфраструктуры после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов инфраструктуры от нарушений работоспособности в случае реализации рассматриваемых угроз, а также:

- определение мер защиты от прерывания обработки информации;
- определение действий по восстановлению работоспособности элементов инфраструктуры в случае прерывания обработки информации.

Действие настоящей Инструкции распространяется на всех должностных лиц Университета, имеющих доступ к ресурсам инфраструктуры, и обеспечивающих непрерывность работы систем:

- защиты от несанкционированного доступа;
- обеспечения отказоустойчивости;
- резервного копирования и восстановления данных;
- контроля физического доступа.

Пересмотр настоящей Инструкции осуществляется по мере необходимости, но не реже одного раза в два года.

2. Порядок реагирования на внештатную ситуацию

2.1. Действия при возникновении внештатной ситуации

В настоящем документе под внештатной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании

элементов, предоставляемых пользователям, а также выявление попыток или фактов несанкционированного доступа (далее – НСД). Внештатной ситуация становится возможной в результате реализации одной из угроз.

Действия администраторов информационных систем в ситуациях, связанных с нарушением целостности информации, повреждения баз данных и нарушения работоспособности информационных систем описываются в документе Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в ФГБОУ ВО «Тольяттинский государственный университет».

Действия системных и сетевых администраторов в нештатных ситуациях регламентируются соответствующими документами Центра новых информационных технологий.

Все действия в процессе реагирования на внештатные ситуации документируются Администратором безопасности в Журнале по учету мероприятий по контролю обеспечения защиты информации. В кратчайшие сроки, не превышающие одного рабочего дня, сотрудники, ответственные за реагирование, и по необходимости другие должностные лица принимают меры по восстановлению работоспособности элементов.

2.2. Действия администраторов подсистем при обнаружении НСД

Если администратор подсистемы, в результате анализа журналов системных событий подозревает или зафиксировал факт НСД, то обязан немедленно сообщить администратору безопасности о событии, с документальным подтверждением факта НСД (скриншоты, копии записей таблиц).

Администратор безопасности совместно с сотрудниками отдела сетевого и системного администрирования ЦНИТ устанавливает:

- факт попытки несанкционированного доступа;

- продолжается ли НСД в настоящий момент;
- источник НСД;
- что является объектом НСД;
- когда происходила попытка НСД;
- как и при каких обстоятельствах была предпринята попытка НСД;
- точка входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД.

Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

- НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;
- проверить не уничтожен ли системный журнал и нет ли в нем пробелов;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки изменения таблиц маршрутизации и адресных таблиц;

- проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

- провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- проверить целостность системных программ;
- проверить систему аутентификации и авторизации.

2.3. Уровни реагирования на инцидент

При реагировании на инцидент, важно правильно классифицировать критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 – Незначительный инцидент.

Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками, согласно регламенту ЦНИТ.

Уровень 2 – Авария.

Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками. В случае аварии к ее устранению привлекаются специалисты соответствующих служб.

К авариям относятся следующие инциденты:

Отказ элементов и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
- отказа системы электропитания;
- сбоя системы кондиционирования.

Уровень 3 – Катастрофа.

Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов и средств защиты, а также к угрозе жизни пользователей, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к работоспособности и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания.

При неблагоприятных природных явлениях, стихийных бедствиях все пользователи выключают свои персональные компьютеры, Администратор сетевого и системного администрирования выключает серверы и сетевое оборудование и принимает меры к эвакуации резервных копий с информацией, жестких дисков содержащих особо ценную информацию.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении внештатных и аварийных ситуаций

3.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства

и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критично важные помещения Университета (помещения, в которых размещаются элементы и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения определяется Регламентом резервного копирования и восстановления работоспособности.

3.2. Организационные меры

Администратор безопасности ознакомляет с данной Инструкцией администраторов подсистем, сетевых и системных администраторов, ответственных за пожарную безопасность, физическую безопасность, энергоснабжение – под подпись в листе ознакомления.

Должно быть проведено обучение администраторов подсистем и должностных лиц, отвечающих за физическую безопасность порядку действий при возникновении внештатных и аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;

- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения, газоснабжения.

Навыки и знания должностных лиц по реагированию на внештатные или аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении внештатной или аварийной ситуации.