СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

ПРАВИЛА РАБОТЫ В ЛОКАЛЬНОЙ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ (ЛИВС) ОИПИ НАН БЕЛАРУСИ

Правила 8.1

Ключевые слова: локальная информационно-вычислительная сеть, эксплуатация, содержание, ремонт, обследование локальной информационно-вычислительной сети, пользователь, права, обязанности, ответственность

ПРЕДИСЛОВИЕ

1 РАЗРАБОТАНО главный инженер, зав. ОРТИ

2 ИСПОЛНИТЕЛИ отдел развития телекоммуникационных инфраструктур (ОРТИ)

3 УТВЕРЖДЕНО И ВВЕДЕНО В ДЕЙСТВИЕ приказом генерального директора от 22.03.2023 № 13-адм.

4 ДОКУМЕНТ СООТВЕТСТВУЕТ законодательству РЕСПУБЛИКИ БЕЛАРУСЬ, а так же требованиям ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ

5 ВВЕДЕНО в замен правил, утвержденных приказом ген. директора ОИПИ НАН Беларуси от 22.12.2015 № 96 - адм

6 ДАТА ВВЕДЕНИЯ 27.03.2023

7 СРОК ДЕЙСТВИЯ постоянно

Издано на русском языке

СОДЕРЖАНИЕ

УТВЕРЖДЕНО
Приказ генерального директора
ОИПИ НАН Беларуси
22.03.2023 № 13-адм.

ПРАВИЛА

Правила 8.1

1 НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

Правила 8.1 работы в локальной информационно-вычислительной сети НАН Беларуси (далее - правила) содержат необходимые требования к ответственным лицам и пользователям по обеспечению работоспособности локальной информационно-вычислительной сети ОИПИ НАН Беларуси (далее - ЛИВС), находящейся в помещениях зданий по ул.Сурганова, 6 и ул.Академической, 25.

2 НОРМАТИВНЫЕ ССЫЛКИ

2.1 Нормативные правовые акты, технические нормативные правовые акты

Настоящие правила разработаны в соответствии с:

1) Конституцией Республики Беларусь 1994 года.

2) Законом Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

3) Законом Республики Беларусь от 17 мая 2011 г. № 262-З «Об авторском праве и смежных правах».

4) Указом Президента Республики Беларусь № 60 от 01 февраля 2010 «О мерах по совершенствованию использования национального сегмента сети Интернет».

5) Уголовным кодексом Республики Беларусь.

6) Гражданским кодексом Республики Беларусь.

2.2 Локальные нормативные правовые акты

В настоящих правилах использованы ссылки на следующие локальные нормативные правовые акты:

1) СТП ОД 03 Управление документацией.

2) СТП ОД 15 Инфраструктура и производственная среда.

3) РСУОТ Руководство по системе управления охраной труда ОИПИ НАН Беларуси.

4) СТП СУОТ 4.3.1Порядок проведения работ по идентификации опасностей, оценке рисков и определение мер управления в области охраны труда.

5) СТП ОД 07 Управление информацией.

6) СТП ОП 08 Управление средствами вычислительной техники и телекоммуникационными сетями.

3 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ, ОБОЗНАЧЕНИЯ

В настоящих правилах используются следующие определения и сокращения:

Администратор ЛИВС – сотрудник отдела РТИ ОИПИ НАН Беларуси, назначенный приказом генерального директора

ДСП – для служебного пользования

ЛИВС – локальная информационно-вычислительная сеть ОИПИ НАН Беларуси

ЛНА – локальные нормативные акты

ОИПИ НАН Беларуси – государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси»

ОРТИ – отдел развития телекоммуникационных инфраструктур

Ответственный по подразделению - руководитель подразделения, либо уполномоченный руководителем подразделения сотрудник в пределах лаборатории/отдела, после согласования с администратором ЛИВС ОИПИ НАН Беларуси. При отсутствии такого назначения ответственным считается руководитель подразделения

ПЗГС – подразделение по защите государственных секретов

ПЭВМ – персональная электронно-вычислительная машина

ТКП – технический кодекс установившейся практики

4 ОБЩИЕ ПОЛОЖЕНИЯ

4.1 Правила содержат необходимые требования к ответственным лицам и пользователям по обеспечению работоспособности ЛИВС, находящейся в помещениях зданий по ул.Сурганова, 6 и ул.Академической, 25.

4.2 Соблюдение данных правил направлено на обеспечение сохранности информации пользователей ЛИВС, контроля ее распространения, а также защиту конфиденциальной и персональной информации пользователей.

4.3 Руководство ОИПИ НАН Беларуси приказом назначает лиц, ответственных за эксплуатацию и развитие ЛИВС ОИПИ НАН Беларуси, выполнение задач по развитию, администрированию ЛИВС и обеспечению информационной безопасности, а также за обучение и консультирование пользователей.

4.4 Управление ЛИВС осуществляется администратором ЛИВС, а также руководителями подразделений, либо уполномоченными руководителями подразделений лицами находящихся в подразделениях ЛИВС, после согласования с администратором ЛИВС.

4.5 Ответственными за администрирование серверов, находящихся в подразделениях ЛИВС, назначаются руководители подразделения, либо лица, назначенные по усмотрению руководителя подразделения, и согласованными с администратором ЛИВС.

5. ПРАВА И ОБЯЗАННОСТИ

5.1 Права администратора ЛИВС ОИПИ НАН Беларуси

Права администратора ЛИВС:

- получать от пользователей сети любую информацию, касающуюся эксплуатируемых ими сетевых ресурсов ЛИВС;
- требовать предоставления доступа в любое помещение, где эксплуатируются сетевые ресурсы ЛИВС;
- собирать любую необходимую информацию о работе сети в статистических целях, а также в целях поддержания безопасности;
- устанавливать на сетевые компьютеры клиентскую часть программ мониторинга;
- осуществлять физический контроль элементов сети и управление поддерживаемых ими сетевых сервисов с целью обеспечения необходимого уровня их надежности и/или защищенности;
- отключать от сети без предварительного уведомления любой сетевой элемент, сетевой сервис, пользователя ЛИВС в случае не соблюдения настоящих правил, повлекшего за собой нарушение системы безопасности или нарушение функционирования ЛИВС, ее элементов и сервисов (подключение элемента сети или сетевого сервиса производится после всестороннего анализа причин и устранения причины отключения).

5.2 Обязанности администратора ЛИВС ОИПИ НАН Беларуси

Обязанности администратора ЛИВС:

- управлять сетью (осуществлять распределение и регистрацию IP-адресов, создание и конфигурирование подсетей и т.п.);
- обеспечивать подключение пользователей к сети;
- осуществлять контроль над функционированием технических средств, образующих ЛИВС;
- локализировать и устранять ошибки в работе сети;
- определить регламенты резервирования и уничтожения информации;
- ежемесячно анализировать уязвимость ЛИВС вирусным атакам;
- нести ответственность за функционирование ЛИВС и её безопасность;
- вопросы системного администрирования ЛИВС решать в контакте с администратором сети BASNET;
- не допускать случаев подключения к ЛИВС организаций, не являющихся абонентами ЛИВС ОИПИ НАН Беларуси, и предоставления им IP-адресов из выделенного для ЛИВС ОИПИ НАН Беларуси адресного пространства;
- обеспечить идентификацию абонентских устройств и пользователей ЛИВС;

- консультировать пользователей ЛИВС в рабочее время;
- предоставлять пользователям учебные и справочные материалы;
- разъяснять пользователям последствия их ошибок;
- содействовать в определении порядка применения средств защиты информации, установленных в подразделениях ЛИВС ОИПИ НАН Беларуси;
- содействовать в определении порядка и перечня используемого программного обеспечения на средствах вычислительной техники сотрудников ОИПИ НАН Беларуси;
- обеспечивать сервис электронной почты на локальном уровне;
- организовывать сопровождение базовых сервисов на серверах;
- обеспечивать доступ к обновлениям операционных систем и антивирусных программных средств.

5.3 Права ответственного по подразделению

Права ответственного по подразделению:
- получать от числящихся в подразделении пользователей сети любую информацию, касающуюся эксплуатируемых ими сетевых ресурсов ЛИВС;
- требовать предоставления доступа в любое помещение, где эксплуатируются сетевые ресурсы подразделения ЛИВС;
- собирать любую необходимую информацию о работе сети в подразделении в статистических целях, а также в целях поддержания безопасности;
- устанавливать на сетевые компьютеры подразделения клиентскую часть программ мониторинга;
- осуществлять физический контроль элементов сети подразделения и управление поддерживаемых ими сетевых сервисов с целью обеспечения необходимого уровня их надежности и/или защищенности, по согласованию с администраторами ЛИВС;
- отключать от сети без предварительного уведомления любой сетевой элемент подразделения, сетевой сервис подразделения, пользователя ЛИВС в случае не соблюдения настоящих правил, повлекшего за собой нарушение системы безопасности или нарушение функциональности ЛИВС, ее элементов и сервисов по согласованию с администраторами ЛИВС (подключение элемента сети или сетевого сервиса производится после всестороннего анализа причин и устранения причины отключения).

5.4 Обязанности ответственного по подразделению

Обязанности ответственного по подразделению:
- ознакомиться с настоящими правилами;
- ознакомить сотрудников подразделения с настоящими правилами;

- зарегистрировать вновь прибывшего пользователя у администратора ЛИВС;

- выполнять работы по сопровождению и развитию своего участка;

- осуществлять управление подключением к подсети с правом приостановления и прекращения доступа, а также контролировать использование ресурсов сети пользователями подразделения по согласованию с администраторами ЛИВС;

- определить регламенты резервирования и уничтожения информации хранящейся в подразделении;

- контролировать производственный характер использования ЛИВС и сети Интернет в подразделении;

- содействовать в организации проведение системного анализа журналов системы защиты информации, предоставляемых уполномоченными поставщиками интернет-услуг по запросу администраторов ЛИВС, государственных органов и подчиненных им государственных организаций;

- содействовать в проведении ежемесячного анализа уязвимостей информационной системы;

- определить порядок применения средств защиты информации, установленных в ЛИВС подразделения;

- определить порядок и перечень используемого программного обеспечения на средствах вычислительной техники сотрудников;

- исключить подключение рабочего места в локальной сети подразделения к сетям связи общего пользования через другие каналы доступа (сотовый телефон, модем);

- нести ответственность за соблюдение политики информационной безопасности, своевременную установку изменений и дополнений к используемым операционным системам и другому программному обеспечению, установленному на серверах подразделения в целях защиты от вирусов и взломов;

- предоставлять администраторам ЛИВС статистические данные по подразделению (списки запрещенных/разрешенных для подразделения сетевых сервисов, адресов).

5.5 Права пользователя ЛИВС ОИПИ НАН Беларуси

Права пользователя ЛИВС:

- получать доступ к имеющимся ресурсам ЛИВС в пределах, разрешенных правилами;

- обращаться за справочной информацией и консультацией к техническому персоналу, обслуживающему технические средства, в пределах их компетенции в рабочее время;

- перед подключением к ЛИВС дополнительных сетевых элементов сообщить об этом администратору ЛИВС;

- получить и использовать канал доступа в глобальную сеть Интернет, а также адрес электронной почты на почтовом сервере;

- установить на пользовательский компьютер резидентные антивирусные программы. Не реже одного раза в неделю обновлять антивирусную базу с сайтов производителей программ-антивирусов и осуществлять комплексную проверку компьютера (разделов дисков, памяти) на наличие вирусов. Проверять на вирусы все данные, импортируемые на компьютер с внешних носителей, электронной почты, полученные из сети т.д. В случае необычного поведения компьютера немедленно сообщить об этом системному администратору ЛИВС.

5.6 Обязанности пользователя ЛИВС ОИПИ НАН Беларуси

Обязанности пользователя ЛИВС:

- выполнять указания и следовать рекомендациям ответственного по подразделению и администратора ЛИВС;

- установить на пользовательский компьютер резидентные антивирусные программы. Не реже одного раза в неделю обновлять антивирусную базу с сайтов производителей программ-антивирусов и осуществлять комплексную проверку компьютера (разделов дисков, памяти) на наличие вирусов. Проверять на вирусы все данные, импортируемые на компьютер с внешних носителей, электронной почты, полученные из сети т.д. В случае необычного поведения немедленно сообщить об этом системному администратору ЛИВС;

- обладать знаниями, необходимыми для работы на компьютерах, включенных в ЛИВС;

- зарегистрироваться в базе данных администратора ЛИВС, заполнив и подписав докладную записку на получение сетевых реквизитов. При этом сообщать администратору ЛИВС только достоверные регистрационные данные, а также сообщать в дальнейшем администратору ЛИВС о любых изменениях в информации, представленной в докладной записке;

- ознакомиться и соблюдать настоящие правила;

- использовать ЛИВС исключительно в производственных целях;

- поддерживать антивирусное программное обеспечение, другие системы безопасности в актуальном состоянии через официальные обновления;

- придерживаться рекомендаций по использованию ресурсов ЛИВС;

- бережно относиться к оборудованию лаборатории (отдела) и оборудованию общего пользования.

5.7 Ограничения для пользователей ЛИВС ОИПИ НАН Беларуси

Пользователю ЛИВС запрещается:

- работать в сети под чужими именем, пользоваться чужими сетевыми реквизитами (IP и/или MAC адресами), допускать коллективное использование, одного и того же имени и пароля;
- проводить работы с информацией ограниченного распространения, а также с грифом ДСП на компьютерах, подключенных к ЛИВС;
- препятствовать ответственному по подразделению и администратору ЛИВС осуществлению своих прав и обязанностей;
- скрывать компьютер из сетевого окружения, отключать режим ответа на запрос исходящего эха (ping);
- предоставлять общий доступ к логическим дискам с правами чтения/записи в случае если это не требуется в рамках выполнения основной деятельности подразделения;
- оставлять свой компьютер, подключенный к ЛИВС, без контроля;
- допускать к подключенному к ЛИВС компьютеру посторонних лиц;
- использовать ЛИВС для угроз и оскорблений;
- использовать программы взлома и подбора паролей пользователей других компьютеров сети;
- использовать на рабочих местах в локальной сети постороннего программного обеспечения, ресурсов сети Интернет, предназначенных для сокрытия действий пользователя, proxy-сервера для получения анонимного доступа к ресурсам сети Интернет (за исключением зарегистрированных в ОИПИ НАН Беларуси сервисов);
- использовать любые программные и аппаратные средства, создающие помехи нормальному функционированию сети, в том числе для фальсификации сообщений электронной почты;
- создавать шлюзы в другие сети передачи данных, сервисы, сети, каналы и системы, в том числе предпринимать попытки перезагрузки систем и широковещательные атаки;
- предпринимать целенаправленные действия по сканированию узлов сетей с целью выявления внутренней структуры сетей, списков открытых портов и т.п.;
- осуществлять неавторизованный перехват, мониторинг, изменение или перенаправление данных и трафика;
- изменять адресную часть и содержимое пакетов данных, создавать виртуальные каналы (тоннели) любого типа и изменять маршрутизацию пакетов;
- создавать ресурсы, скачивать информацию, содержащую материалы противоречащие законодательству Республики Беларусь, и направленные на:

1) осуществление экстремистской деятельности;

2) незаконный оборот оружия, боеприпасов, взрывных устройств, взрывчатых, радиоактивных, отравляющих, сильнодействующих, ядовитых, токсических веществ, наркотических средств, психотропных веществ и их прекурсоров;

3) содействие незаконной миграции и торговле людьми;

4) распространение порнографических материалов;

5) пропаганду насилия, жестокости и других деяний, запрещенных законодательством;

6) размещать и скачивать из сети Интернет литературные, научные, музыкальные, фотографические, аудиовизуальные произведения, произведения изобразительного искусства, программные средства и иные объекты авторского права и смежных прав, пользующихся правовой охраной на территории Республики Беларусь, без согласия их правообладателей (если иное не определено законодательными актами) и при условии соблюдения иных требований законодательства об авторском праве и смежных правах;

7) размещать и распространять в сети Интернет информационные сообщения и (или) материалы, заимствованные с информационного ресурса информационного агентства, иного средства массовой информации, распространяемого через сеть Интернет, только с использованием адресации (гиперссылки) на первоисточник информации и (или) средство массовой информации, ранее распространившее эти информационные сообщения и (или) материалы, если обладателем таких сообщений и (или) материалов не установлены иные условия их распространения;

- устанавливать сетевое программное обеспечение без согласования с ответственным по подразделению либо администратором подсети подразделения;

- использовать компьютер в сети при наличии на нем вирусов. При обнаружении вируса пользователь должен немедленно отключить компьютер и обратиться к системному администратору;

- использовать IP-телефонию, публичные системы мгновенных сообщений (ICQ, Skype и т.д.), а также осуществлять доступ к социальным сетям («Одноклассники», «В контакте» и др.) без производственной необходимости;

- использовать ЛИВС для передачи информации, не имеющей отношения к научной и производственной деятельности института: (компьютерных игр, видеоклипов, бесед на отвлеченные темы и т. п.);

- разрабатывать или распространять любые виды компьютерных вирусов, «троянских коней», «логических бомб» и других информационных угроз;

- выключать и включать любое компьютерное и сетевое оборудование общего пользования и производить переключение внешних соединений такого оборудования;

- производить тестирование и поиск способов нарушения или преодоления систем контроля доступа к ресурсам сети (компьютеру; маршрутизатору, другому оборудованию или информационному ресурсу), последующее использование такого доступа, а также уничтожение или модификацию программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами этого программного обеспечения или данных. Под несанкционированным доступом понимается любой доступ, осуществляемый способом, отличным от предполагавшегося владельцем ресурса или зарегистрированным на BASNET;

- создавать в ЛИВС публичные Web, Ftp, Mail, DHCP и другие серверы без согласования с администратором ЛИВС;

- монополизировать ресурсы ЛИВС, блокируя работу других пользователей;

- осуществлять коммерческое использование ЛИВС и ее информационных ресурсов;

- передавать сведения, полученные в ходе научно-производственной деятельности, подлежащие защите и составляющие государственную тайну Республики Беларусь;

- использовать ЛИВС для деятельности, противоречащей национальным интересам Республики Беларусь.

5.8 Ответственность пользователя ЛИВС ОИПИ НАН Беларуси

5.8.1 Самовольное подключение к сети и использование пользователем сетевых реквизитов, ему не принадлежащих, является серьёзнейшим нарушением правил. Установление подобного факта влечёт за собой проведение служебного расследования и принятие мер дисциплинарного (административного) воздействия к нарушителю и руководителю подразделения, подтвердившему полномочия данного пользователя сети при получении сетевых реквизитов.

5.8.2 Нарушители несут ответственность в соответствии с Гражданским, Административным и Уголовным кодексами Республики Беларусь.

Гарантом корректной работы пользователя в сети выступает руководитель подразделения (зав. лабораторией, зав. отделом), в котором работает пользователь.

6 ПОРЯДОК РЕГИСТРАЦИИ И РАБОТА ПОЛЬЗОВАТЕЛЕЙ ЛИВС ОИПИ НАН БЕЛАРУСИ

6.1 Любой пользователь ЛИВС, использующий в своей работе компьютер с установленным сетевым адаптером, имеет право подключаться к оборудованию общего пользования при условии соблюдения настоящих правил.

6.2 Регистрация пользователей в сети производится на основании докладной записки заведующего подразделением на имя главного инженера ОИПИ НАН Беларуси.

6.3 При регистрации в сети администратор сети создает имя пользователя (nickname), временный регистрационный пароль и определяет его права и привилегии, что позволяет пользователю использовать сетевые сервисы. Пользователю присваивается уникальный ip-адрес на основании mac-адреса предоставленного ответственным по подразделению в докладной записке.

6.4 Изменение прав и привилегий пользователя осуществляется только администратором сети.

6.5 Пользователь защищает свои права и привилегии паролем и меняет его в соответствии с регламентом принятым в подразделении. Защита пароля от разглашения обеспечивается пользователем.

6.6 Требования к паролю

- пароль должен содержать символы минимум трех из следующих четырех категорий:
- прописные символы латиницы (от A до Z);
- строчные символы латиницы (от a до z);
- цифры (от 0 до 9);
- небуквенные символы (например, !, $, #, %);
- длина пароля должна быть не менее 8 символов;
- пароль не должен включать в себя:
- легко вычисляемые сочетания символов (имена, фамилии, известные названия, слова русского или английского языка, в том числе слова без гласных или согласных букв словарные и жаргонные слова и т.д.);
- упорядоченные последовательности символов и знаков (111, qwerty, abcd и т.д.), последовательности символов в соответствии с раскладкой клавиатуры;
- общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), а также имя или часть имени учетной записи пользователя;
- аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- повтор слов, обратный порядок букв в слове;

- при формировании пароля запрещается использовать транслитерацию букв (замена букв в слове буквами другого алфавита) и другую раскладку клавиатуры.

При вводе пароля в процессе аутентификации значения символов пароля отображаются на экране монитора в скрытом виде (в виде символов «*»).

Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

Запрещается сообщать другим пользователям личный пароль и идентификатор.

Запрещается регистрироваться и работать в ЛИВС под чужим идентификатором и паролем.

7 РЕКОМЕНДАЦИИ ПО ВЫБОРУ ПАРОЛЯ

7.1 Необходимо, чтобы пользователи выбирали себе сложные пароли, не поддающиеся простой программной расшифровке. В случае если у пользователя возникло подозрение, что его пароль стал известен другим лицам, он должен незамедлительно сменить его или обратиться к администратору сети с просьбой о смене пароля.

7.2 Хороший пароль — легкий для запоминания, но неочевидный для хакера, который невозможно взломать с помощью программных средств. Хороший пароль должен быть уникальным и комбинированным. Ниже перечислены некоторые рекомендации по созданию надежных паролей:

- используйте буквы верхнего и нижнего регистра, специальные символы и цифры;
- не используйте такие пароли, как «123456», слово «password» или любые другие аналогичные пароли с низкой защитой;
- длина пароля должна составлять не менее восьми символов. Чем длиннее пароль, тем труднее его подобрать;
- не используйте отдельные слова из разных языков. Для взлома таких паролей хакеры используют атаку по словарю;
- рекомендуется создавать бессмысленные и случайные пароли;
- не используйте производные собственного имени, имен родственников или домашних животных;
- создавать разные пароли для каждой учетной записи;
- никогда не записывать пароли и не сообщать их никому;
- регулярно менять пароли;
- не сохранять пароли в браузере, держать пароль в памяти или хранить его в специальной программе, предназначенной для управления паролями. В состав программ по обеспечению безопасности Norton Internet Security и Norton 360 входит инструмент Norton Identity Safe, обеспечивающий безопасное хранение паролей и их подстановку в веб-формах в зашифрованном виде;
- создавать фразу-пароль, которую можно немного изменить для каждого веб-сайта. Пример такой фразы: «I want to go to England». Затем создайте аббревиатуру, состоящую из первых букв каждого слова этой фразы, и замените слово "to" цифрой "2". Таким образом, вы получите следующий пароль: iw2g2e. Затем добавьте первую и последнюю букву в названии веб-сайта для создания нового пароля. Например, для веб-сайта Norton.com новый уникальный и комбинированный пароль будет выглядеть следующим образом - Niw2g2en. Преимуществом таких фраз-паролей является простота запоминания, использование личных фактов и возможность модификации для создания уникального пароля для каждого веб-сайта.

8 ПОРЯДОК ИСПОЛЬЗОВАНИЯ РЕСУРСОВ ЛИВС ОИПИ НАН БЕЛАРУСИ

8.1 Ресурсы ЛИВС могут использоваться только в целях, соответствующих направлениям научной деятельности ОИПИ НАН Беларуси, включенным в тематический план института, а также в целях обеспечения условий для выполнения этих работ. Другое использование ресурсов ЛИВС должно регламентироваться администрацией ОИПИ НАН Беларуси индивидуально.

8.2 Все подключения, отключения, переключения и перенастройки сетевых элементов производятся сотрудниками ОРТИ либо персоналом отдела телекоммуникации академсети, если это не противоречит условиям ввода в эксплуатацию этих элементов.

8.3 Доступ, непосредственный или удаленный, к оборудованию общего пользования разрешается только зарегистрированным участникам сети. Отключение участником сети электропитания любого оборудования общего пользования допускается только в экстренных ситуациях (пожар, дым из оборудования, затопление оборудования водой и т.п.), т.е. в случаях, предусмотренных действующими инструкциями ОИПИ НАН Беларуси, связанными с обеспечением пожарной безопасности при проведении работ и сохранностью оборудования.

9 ЭКСПЛУАТАЦИЯ СЕТЕВОГО ОБОРУДОВАНИЯ И КАБЕЛЬНЫХ ЛИНИЙ ЛИВС ОИПИ НАН БЕЛАРУСИ

9.1 Все работы, связанные с прокладкой, коммутацией и обслуживанием кабельных линий ЛИВС, а также установкой и настройкой сетевого оборудования выполняются:

- ЛИВС по адресу ул.Сурганова, 6 - персоналом ОРТИ;
- ЛИВС по адресу ул.Академическая, 25 - персоналом отдела телекоммуникации академсети.

9.2 Пользователям ЛИВС категорически запрещается самостоятельно выполнять коммутацию кабельных соединений персональных компьютеров, подключенных к ЛИВС, а также производить все виды работ по конфигурированию и установке сетевого оборудования (за исключением п. 5,7).

9.3 В случаях повреждения кабельных линий и сетевого оборудования ЛИВС по вине пользователя всю полноту ответственности за причиненный ущерб несет пользователь и руководитель подразделения (зав. лабораторией, зав. отделом), в котором работает пользователь.

10 ИНСТРУКЦИЯ ПО ОБРАБОТКЕ ВХОДЯЩЕЙ И ИСХОДЯЩЕЙ ЭЛЕКТРОННОЙ ПЕРЕПИСКИ

10.1 Электронная почта (e-mail) является одной из сервисных услуг, предоставляемых пользователям ЛИВС, и предназначена для передачи или получения корреспонденции по компьютерным сетям.

10.2 Прием (передача) корреспонденции осуществляется только с пользовательских компьютеров, установленных в подразделениях, через почтовые сервера, установленные на узлах электронной почты ОИПИ НАН Беларуси в помещениях зданий по ул.Сурганова, 6 и ул.Академическая, 25.

10.3 Регистрация абонентов e-mail осуществляется администраторами ЛИВС и производится на основании докладной записки руководителя подразделения на имя главного инженера института с обоснованием необходимости использования электронной почты (приложение А). При регистрации абонент должен ознакомиться с настоящими правилами.

10.4 Корреспондентам e-mail института предоставлена возможность бесплатного пользования электронной почтой только для переписки в рамках производственной и научной деятельности. Размер почтового ящика не более 100 МБ.

10.5 Для уменьшения размера электронных сообщений и объединения нескольких вложенных файлов в один, а также исключения использования в качестве вложения исполняемых файлов (типа .exe; .bin; .cmd; .gadget; и.т.п.) рекомендуется использовать программы для сжатия (компрессии) вложенных документов. Абонент e-mail несет персональную ответственность за содержание передаваемой им корреспонденции, т. е. за информацию:

- полученную в ходе научно-производственной деятельности;
- подлежащую защите;
- составляющую государственную тайну Республики Беларусь.

При этом должны соблюдаться общепринятые морально-этические и правовые нормы.

10.6 Для получения иных видов услуг приема-передачи информации пользователи могут обратиться за консультацией к администратору ЛИВС.

10.7 При работе с электронной почтой запрещается:

- использовать корпоративную электронную почту не в производственных целях;
- производить рассылку материалов рекламного (непрофильного) и развлекательного характера;
- производить массовую рассылку писем непроизводственного характера;
- пересылать исполняемые файлы (с расширениями - .exe; .bin; .cmd; .gadget; и.т.п.) как потенциальные источники информационных угроз;

- пересылать мультимедийные файлы (аудио и видео), а также другую информацию не связанную с производственной деятельностью;

- производить рассылку вредоносных программ или файлов, зараженных вирусами;

- использовать электронную почту для передачи материалов большого объема (более 30 МБ);

- передавать сторонним лицам почтовые аккаунты, публиковать свой корпоративный e-mail адрес, либо адреса других работников компании на общедоступных Интернет ресурсах (форумы, конференции и т.п.);

- пересылать по электронной почте пароли к каким бы то ни было ресурсам ЛИВС;

- открывать вложения к сообщениям электронной почты, полученным из неизвестных, подозрительных или ненадежных источников. Такие вложения должны незамедлительно удаляться;

- несанкционированное использования e-mail для получения видов услуг или услуг, которые могут повлечь за собой финансовые расходы института (использование платных услуг, предоставляемых различными сайтами в Интернете и т.п.). Ответственность за подобный инцидент и оплату полученных услуг несет сам абонент, а также руководитель подразделения, в котором это произошло. Абонент при этом лишается возможности работать в ЛИВС до момента окончания проведения служебного расследования и принятия мер дисциплинарного, административного воздействия к нарушителю и его руководителю подразделения и осуществления полного расчета за полученные услуги.

10.8 В целях предотвращения заражения операционной системы вредоносными программами (вирусами) рекомендуется с повышенной внимательностью и осторожностью относиться к входящим письмам если:

- входящее письмо получено от неизвестного ранее адресата (подписано неизвестным или, наоборот, известным лицом (организацией), с которым переписка ранее не велась: MeganFox@, KRonaldo@, EADS@ и т.д., Наличие цифр в имени почтового ящика или почтового сервиса - дополнительный сигнал для классификации его как подозрительного.).

- почтовый адрес отправителя размещен на бесплатных, не требующих ввода при регистрации телефонного номера или на вымышленных почтовых сервисах (@yandex.ru/com, @63x423.mailmarket.ru, @se8t5ghz.mailmarket.ru, @alrayan.com, Jlopez@gracephoto.com).

- в письме от незнакомого пользователя присутствует следующая информация:

а) указываются временные параметры, требующие принятия срочного решения (количество дней или часов; обороты: «срочно», «как можно быстрее», «не терпит отлагательств» и т.д.);

б) наличие у отправителя каких-либо проблем со связью с

получателем (то есть объяснение того, что получатель не знает, с кем имеет дело), с выполнением работ, с отправкой грузов, с получением документов и т.д.;

в) описывается проблемный вопрос материального характера (денежная транзакция, поставки/закупки, создание инвестиционных фондов, денежный выигрыш, пожертвование и т.д.);

г) основная масса писем с вредоносным программным обеспечением содержит вложенные файлы с расширениями doc/docx, xls/xlsx, rtf, pdf, jpg, jpeg, zip, rar и exe;

д) в письме от незнакомого отправителя имеется пароль для доступа к такому файлу, не следует открывать вложенный файл и вводить указанную комбинацию цифр;

- файлы с расширением .exe открывать запрещено;

- письма содержащие ссылки HTML, осуществлять переход по которым (даже от известных отправителей) не рекомендуется (всю необходимую информацию они могут переслать сами). Письмо может быть написано шрифтом другого цвета, в тексте которого часто размещается такая ссылка, поэтому не рекомендуется кликать по тексту данного письма.

11 ИНСТРУКЦИЯ ПО РАБОТЕ С FLASH НАКОПИТЕЛЯМИ

11.1 В случае необходимости использования сменных внешних накопителей, пользователь ЛИВС обязан поставить в известность ответственного по подразделению, а так же провести проверку этих носителей на отсутствие «вирусов».

11.2 Исключить хранение на flash-накопителе, в период его подключения к ПЭВМ, имеющей доступ к сети Интернет, электронных документов непланируемых к обработке на данной ПЭВМ.

11.3 Используя средства шифрования (TrueCrypt и т.п.) создать из flash-накопителя крипто контейнер, не позволяющий использовать указанный накопитель в неслужебных целях.

11.4 Организовать ежемесячное форматирование flash-накопителей.

11.5 Исключить использование flash-накопителей во время противодействия выявленному вредоносному программному обеспечению.

12 ВНЕСЕНИЕ ИЗМЕНЕНИЙ

12.1 Внесение изменений в настоящие правила осуществляется согласно СТП ОД 03 [2.2; 1].

12.2 Внесение изменений в настоящие правила осуществляется с разрешения гл. инженера и ведущего специалиста ПЗГС.

12.3 Гл. инженер один раз в три года пересматривает данные правила на актуальность и соответствие требованиям ТКП. По итогам рассмотрения принимается решение о продлении действия правил без изменений. В этом случае действие правил продлевается на следующие три года, для чего ведущий инженер по качеству делает запись в «Листе регистрации изменений» контрольного экземпляра: Срок действия продлен до 20__ г., расписывается и ставит дату. В противном случае делается запись: Требует пересмотра. Срок действия продлен до 20__ г. (срок продления в этом случае не должен превышать один месяц), расписывается и ставит дату. Такая запись инициирует начало пересмотра данных правил.

ПРИЛОЖЕНИЕ А
(справочное)

Бланк докладной записки для предоставления сетевых реквизитов

Государственное научное учреждение
«Объединенный институт проблем
информатики Национальной академии
наук Беларуси» (ОИПИ НАН Беларуси)

Главному инженеру
ОИПИ НАН Беларуси
Максимову В.В.

Лаборатория (отдел) №_____

ДОКЛАДНАЯ ЗАПИСКА

«____» _____ 20__ г.

г. Минск

О предоставлении сетевых реквизитов

От _____
(Ф.И.О. заведующего лабораторией / отделом)

Прошу предоставить сетевые реквизиты для работы в ЛИВС ОИПИ НАН Беларуси компьютеру/сетевому оборудованию, расположенному в отделе (лаборатории)

mac-адрес оборудования: _____:_____:_____:_____:_____:_____
(Пуск->Выполнить->cmd->ipconfig /all)

Ф.И.О. пользователя: _____
(полностью)

Заведующий лабораторией (отделом) _____
(подпись)

С правилами работы
ЛИВС ОИПИ НАН Беларуси _____ _____
(Ознакомлен) **(Подпись пользователя)**

СОГЛАСОВАНО
Администратор ЛИВС ОИПИ НАН Беларуси (к.211) _____
(Подпись)

(далее заполняется администратором ЛИВС ОИПИ НАН Беларуси)

Выделены:
IP-адрес v4: _____/_____/_____/_____

IP-адрес v6: _____/_____/_____/_____/_____/_____/_____/_____

E-mail адрес: _____@newman.bas-net.by

ПРИЛОЖЕНИЕ Б
(справочное)

Общая информация о вирусных угрозах

Б1 Классификация вредоносных программ

Одних только типов вредоносных программ известно великое множество. Но каждый тип состоит из огромного количества образцов, также отличающихся друг от друга. Для борьбы со всеми ними нужно уметь однозначно классифицировать любую вредоносную программу и легко отличить ее от других вредоносных программ.

Б2 Дерево классификации вредоносных программ

Общепринятая система классификации четко описывает каждый обнаруженный объект и назначает конкретное местоположение в дереве классификации, показанном ниже. На диаграмме «Дерево классификации»:

- типы поведения, представляющие наименьшую опасность, показаны в нижней области диаграммы;
- типы поведения с максимальной опасностью отображаются в верхней части диаграммы Б1.

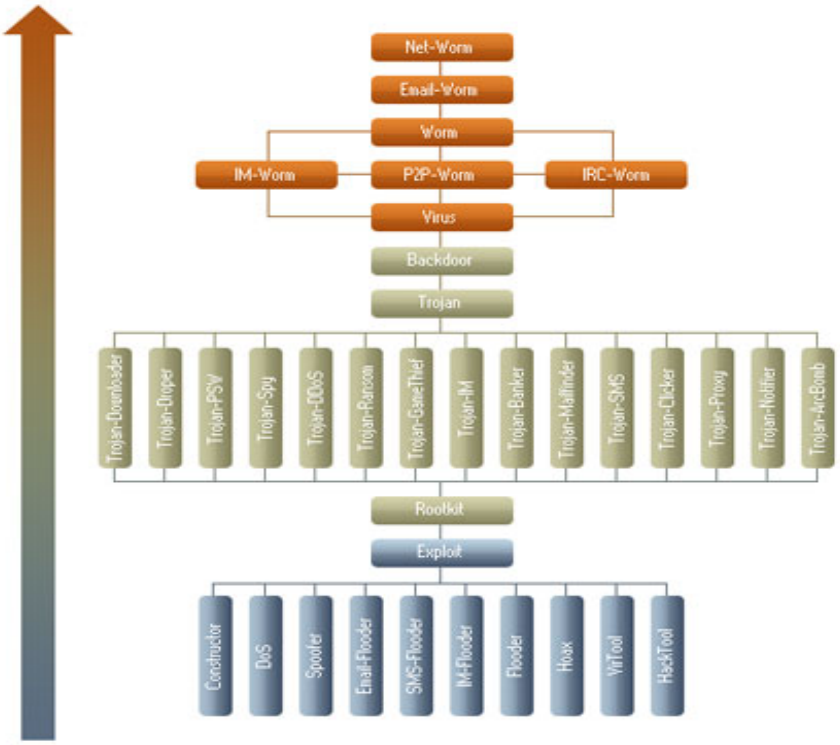

Диаграмма Б1- Дерево классификации

Б3 Многофункциональные вредоносные программы

Отдельные вредоносные программы часто выполняют несколько вредоносных функций и используют несколько способов распространения, без некоторых дополнительных правил классификации это могло бы привести к путанице.

Например: существует вредоносная программа, которая занимается сбором адресов электронной почты на зараженном компьютере без ведома пользователя. При этом она распространяется как в виде вложений электронной почты, так и в виде файлов через сети P2P. Тогда программу можно классифицировать и как Email-Worm, и как P2P-Worm или Trojan-Mailfinder. Чтобы избежать такой путаницы, применяется набор правил, которые позволяют однозначно классифицировать вредоносную программу по конкретному поведению, независимо от второстепенных свойств.

На диаграмме Б1 видно:

- что каждому поведению назначен свой уровень опасности;
- поведения, представляющие собой большую опасность, расположены выше тех видов, которые представляют меньшую опасность.

И поскольку в нашем примере поведение Email-Worm представляет более высокий уровень опасности, чем поведение P2P-Worm или Trojan-Mailfinder, вредоносную программу из нашего примера можно классифицировать как Email-Worm.

Б4 Несколько функций с одинаковым уровнем опасности

Если вредоносная программа имеет несколько функций с одинаковым уровнем опасности (таких как Trojan-Ransom, Trojan-ArcBomb, Trojan-Clicker, Trojan-DDoS, Trojan-Downloader, Trojan-Dropper, Trojan-IM, Trojan-Notifier, Trojan-Proxy, Trojan-SMS, Trojan-Spy, Trojan-Mailfinder, Trojan-GameThief, Trojan-PSW или Trojan-Banker), она классифицируется как троянская программа.

Если у вредоносной программы есть несколько функций с одинаковым уровнем опасности, таких как IM-Worm, P2P-Worm или IRC-Worm, она классифицируется как червь.

Б5 Что такое компьютерный вирус и компьютерный червь

Компьютерный вирус и компьютерный червь – это вредоносные программы, которые способны воспроизводить себя на компьютерах или через компьютерные сети. При этом пользователь не подозревает о заражении своего компьютера. Так как каждая последующая копия вируса или компьютерного червя также способна к самовоспроизведению, заражение распространяется очень быстро.

Существует очень много различных типов компьютерных вирусов и компьютерных червей, большинство которых обладают высокой способностью к разрушению.

Б6 Что нужно знать о компьютерных вирусах и червях

Вредоносное программное обеспечение из подкласса вирусов и червей включает:

- Email-Worm;
- IM-Worm;
- IRC-Worm;
- Net-Worm;
- P2P-Worm;
- Virus.

Б7 Компьютерные черви

Большинство известных компьютерных червей распространяется следующими способами:

- в виде файла, отправленного во вложении в электронном письме;
- в виде ссылки на интернет - или FTP-ресурс;
- в виде ссылки, переданной через сообщение ICQ или IR;
- через пиринговые сети обмена данными P2P (peer-to-peer);
-некоторые черви распространяются как сетевые пакеты. Они проникают прямо в компьютерную память, затем активируется код червя.

Компьютерные черви могут использовать ошибки конфигурации сети (например, чтобы скопировать себя на полностью доступный диск) или бреши в защите операционной системы и приложений. Многие черви распространяют свои копии через сеть несколькими способами.

Б8 Вирусы

Вирусы можно классифицировать в соответствии с тем, каким способом они заражают компьютер:

- файловые вирусы;
- вирусы загрузочного сектора;
- макровирусы;
- вирусные скрипты.

Любая программа данного подкласса вредоносного программного обеспечения в качестве дополнительных может иметь и функции троянской программы.

Б9 Троянская программа

Троянские программы – это вредоносные программы, выполняющие несанкционированные пользователем действия. Такие действия могут включать:

- удаление данных;
- блокирование данных;
- изменение данных;
- копирование данных;
- замедление работы компьютеров и компьютерных сетей

В отличие от компьютерных вирусов и червей троянские программы неспособны к самовоспроизведению.

Б10 Что нужно знать о троянских программах

Троянские программы классифицируются в соответствии с типом действий, выполняемых ими на компьютере.

– **Бэкдоры** - троянская программа бэкдор предоставляет злоумышленникам возможность удаленного управления зараженными компьютерами. Такие программы позволяют автору выполнять на зараженном компьютере любые действия, включая отправку, получение, открытие и удаление файлов, отображение данных и перезагрузку компьютера. Троянцы-бэкдоры часто используются для объединения группы компьютеров-жертв в ботнет или зомби-сеть для использования в криминальных целях.

– **Эксплойты** - это программы с данными или кодом, использующие уязвимость в работающих на компьютере приложениях.

– Руткиты - это программы, предназначенные для сокрытия в системе определенных объектов или действий. Часто основная их цель - предотвратить обнаружение вредоносных программ, чтобы увеличить время работы этих программ на зараженном компьютере.

– **Банковские троянцы** (Trojan-Banker) предназначены для кражи учетных данных систем интернет-банкинга, систем электронных платежей и кредитных или дебетовых карт.

– **DDoS-троянцы -** эти программы предназначены для проведения атак типа «отказ в обслуживании» (Denial of Service, DoS) по целевым веб-адресам. При такой атаке с зараженных компьютеров системе с определенным адресом отправляется большое количество запросов, что может вызвать ее перегрузку и привести к отказу в обслуживании.

– Программы **Trojan-Downloader** способны загружать и устанавливать на компьютер-жертву новые версии вредоносных программ, включая троянские и рекламные программы.

– **Trojan-Dropper** - эти программы используются хакерами, чтобы установить троянские программы и/или вирусы или предотвратить обнаружение вредоносных программ. Не каждая антивирусная программа способна выявить все компоненты троянских программ этого типа.

– Программы типа **Trojan-FakeAV** имитируют работу антивирусного программного обеспечения. Они созданы, чтобы вымогать деньги у пользователя в обмен на обещание обнаружения и удаления угроз, хотя угроз, о которых они сообщают, в действительности не существует.

– **Игровые троянцы** - программы этого типа крадут информацию об учетных записях участников сетевых игр.

– Программы **Trojan-IM** крадут логины и пароли к программам мгновенного обмена сообщениями, таких как ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и многие другие.

– **Trojan-Ransom** - троянские программы этого типа могут изменить данные на компьютере таким образом, что компьютер перестает нормально работать, а пользователь лишается возможности использовать определенные данные. Злоумышленник обещает восстановить нормальную работу компьютера или разблокировать данные после уплаты запрашиваемой суммы.

– **SMS-троянцы** - отправляют текстовые сообщения с мобильного устройства на платные телефонные номера с повышенным тарифом, тратя ваши деньги.

– **Шпионские программы** типа Trojan-Spy способны скрыто наблюдать за использованием компьютера, например, отслеживая вводимые с клавиатуры данные, делая снимки экрана и получая список работающих приложений.

– **Trojan-Mailfinder** - такие программы способны собирать на вашем компьютере адреса электронной почты.

Также встречаются другие виды троянских программ:

- Trojan-ArcBomb;
- Trojan-Clicker;
- Trojan-Notifier;
- Trojan-Proxy;
- Trojan-PSW.

Б11 Вредоносные утилиты

Вредоносные утилиты – это вредоносные программы, предназначенные для автоматизации создания вирусов, червей или троянских программ, DoS-атак на удаленные серверы, взлома других компьютеров и т.п.

Б12 Что нужно знать о вредоносных утилитах

В отличие от вирусов, червей и троянских программ, вредоносные утилиты сами не представляют угрозы для компьютера, на котором исполняются, а вредоносные действия выполняются приложением только по прямому указанию злоумышленника.

Б13 Виды шпионского программного обеспечения

Категория Adware, Pornware и Riskware включает легально разработанные программы, которые в определенных случаях могут представлять особую опасность для пользователей компьютеров (действуя так же, как шпионское программное обеспечение).

Хотя многие из таких программ, вероятно, разработаны и распространяются легальными компаниями, они могут иметь функции, которые используются некоторыми создателями вредоносных программ во вредоносных или незаконных целях.

Б14 Условия для распространения вредоносных программ

Вредоносное программное обеспечение может атаковать операционные системы или приложения, если операционные системы или приложения способны выполнять программы, которые не входят в их состав. Такая возможность есть у всех популярных операционных систем для настольных компьютеров и многих офисных приложений, графических редакторов и программ для дизайна, а также других программных сред со встроенными языками сценариев.

Поэтому все такие популярные операционные системы и приложения уязвимы для атак вредоносных программ.

Б15 Не все операционные системы и приложения подвергаются атакам

Компьютерные вирусы, черви и троянские программы написаны для очень многих операционных систем и приложений. Однако существуют другие операционные системы и приложения, для которых вредоносные программы еще не обнаружены. Какова разница между этими двумя группами операционных систем и приложений?

Б16 Три условия, которые необходимы для появления и распространения вредоносных программ

Обычно вредоносная программа для каждой конкретной операционной системы или приложения появляется при соблюдении следующих трех условий:

- скорость внедрения и популярность операционной системы;
  операционная системы широко используется
- доступность документации;
  существует подробная документация по операционной системе
- наличие уязвимостей и эксплойтов к ним;
  операционная система не защищена или есть известные уязвимости в операционной системе или приложении.

Б17 Кто создает вредоносные программы

Если вы не можете понять, зачем кто-то прилагает столько усилий, чтобы атаковать ваш компьютер или ваше мобильное устройство, давайте попробуем рассмотреть, что за люди пишут вредоносные программы и как они зарабатывают на создании вредоносных программ.

Б18 Компьютерные хулиганы, мошенники, шантажисты и другие преступники

Печально, но рано или поздно злоумышленники находят, как воспользоваться практически любыми изобретениями или новыми технологиями, чтобы причинить вред устройству или извлечь выгоду. По мере роста использования компьютеров, мобильных устройств и интернета создание компьютерных вирусов, червей, троянских программ и другого вредоносного программного обеспечения становится все более выгодным для хулиганов, мошенников, шантажистов и других преступников. И чем больше появляется устройств, тем шире становятся возможности киберпреступников.

Б19 Ущерб, который наносят вредоносные программы

Вирусы, черви и троянские программы могут нанести вред компьютерам, сетям, мобильным устройствам и данным.

Возможные последствия заражения вредоносными программами для домашних и корпоративных пользователей

Масштаб ущерба, причиненного вредоносной программой, зависит от того, что подверглось заражению: домашний компьютер или корпоративная сеть. Размер ущерба также зависит от конкретного типа вредоносной программы и типа зараженного устройства, а также от характера данных, которые хранились на устройстве или были оттуда доступны.

В одних случаях последствия заражения вредоносными программами незначительны, в других они могут иметь весьма серьезный характер.

- Для домашних пользователей заражение может повлечь утрату не слишком ценных данных, которые легко восстановить, или привести к

раскрытию информации, например предоставляющей киберпреступникам доступ к банковскому счету пользователя.

- В корпоративной сети троянец, рассылающий спам, может вызвать незначительное увеличение почтового трафика, тогда как другие виды заражения могут привести к нарушению работы корпоративной сети или потере критически важных для бизнеса данных.

Б20 Как защититься от компьютерных вирусов и червей

Рекомендуется установить антивирус: программное обеспечение для защиты от вредоносных программ на все свои устройства (включая ПК, ноутбуки, компьютеры Mac и смартфоны). Решение для защиты от вредоносных программ должно регулярно обновляться, чтобы защищать от самых последних угроз.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ изм.	Дата изменения	Содержание изменения	Основание для изменения	№ страницы

ЛИСТ СОГЛАСОВАНИЯ

Наименование СП, должность	Ф.И.О.	Подпись	Дата
1	**2**	**3**	**4**
Зам. ген. директора по научной работе	Касанин С.Н.		
Гл. инженер	Максимов В.В.		
Зав. ОРТИ	Мицкевич А.А.		
Вед. инженер	Драчиловский А.Г.		
Техник 1 категории	Странаков В.А.		
Вед. инженер по качеству	Аманенко В.В.		

ЛИСТ РАССЫЛКИ

№ экз.	Обозначение	Изменения	Место хранения	Ф.И.О. получателя	Дата	Подпись
1	2	3	4	5	6	7