ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

г. Улан-Удэ, 2011 г.

Содержание

Термины и определения

Администратор безопасности информационных систем - работник, обеспечивающий исполнение мер по информационной безопасности;

Атака – несанкционированная деятельность с вредоносными намерениями, использующая специально разработанный программный код или специальные методики;

Аутентификация - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа реализованными в системе;

Авторизация – определение по данным аутентификации полномочий лица или информационного ресурса и элементов, к которым им следует предоставить доступ;

База данных (БД) - упорядоченная совокупность данных и структур их хранения, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, и предназначенная для обработки с помощью средств вычислительной техники;

Вероятность реализации угрозы через данную уязвимость - степень возможности реализации угрозы через данную уязвимость в тех или иных условиях;

Вредоносное программное обеспечение – программное обеспечение, создаваемое с целью причинения вреда информационным системам и информационным ресурсам;

Защита информации - принятие правовых, организационных и технических (программно-технических) мер в целях обеспечения целостности сохранности информации, недопущения ее несанкционированного изменения или уничтожения, соблюдения конфиденциальности информации ограниченного доступа, реализации права на доступ к информации, а также недопущения несанкционированного воздействия на средства обработки, передачи и хранения информации;

Защита информации от несанкционированного *доступа* - меры, направленные на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными правовыми актами или собственником, владельцем информации прав или правил доступа к ней;

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиям, устанавливаемыми собственником информации, которыми может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо;

Защита программных средств - организационные, правовые, технические и технологические меры, направленные на предотвращение возможных

несанкционированных действий по отношению к программным средствам и устранение последствий этих действий;

Идентификатор - уникальный персональный код, присвоенный субъекту и объекту системы, предназначенный для регламентированного доступа к системе и ресурсам системы;

Идентификация - определение соответствия предъявленного для получения доступа в систему, к ресурсу идентификатора перечню идентификаторов, имеющихся в системе;

Несанкционированный доступ к информации – получение защищаемой информации, заинтересованным субъектом, с нарушением установленных правовыми документами правил доступа к ней;

Несанкционированный доступ к программным средствам - доступ к программам, записанным в памяти ЭВМ или на машинном носителе, а также отраженным в документации на эти программы, осуществленный с нарушением установленных правил;

Пользователь - человек, организация, система, использующие в своей работе в той или иной мере компьютер, вычислительную систему, базу данных, сеть и пр. Очень широкое понятие, которое может заменять понятия: оператор, программист, абонент и т.д.;

Доступ - перемещение людей, транспорта и других объектов в (из) помещения, здания, зоны и территории;

Разграничение доступа - порядок доступа лиц к техническим и программным средствам, защищаемой информации при ее обработке на средствах вычислительной техники в соответствии с заранее разработанными и утвержденными правилами*;*

Рабочее место – оборудованное *рабочее место пользователя (администратора)* — стол, стул, компьютер, с установленными необходимыми ПО;

Рабочая станция – комплекс технических и программных средств предназначенных для решения определенного круга задач;

Система обеспечения информационной безопасности – система мер направленная на выявление угроз информационной безопасности, предотвращения и пресечения их реализации, а также ликвидации последствий реализованных в результате НСД;

Средства вычислительной техники – совокупность программных и технических элементов систем обработки информации, способных функционировать самостоятельно или в составе других систем;

Средства защиты информации – технические, криптографические, программные и другие средства, вещества или материалы, предназначенные или используемые для

защиты информации;

Средства криптографической защиты информации – средства, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности;

Средства обеспечения информационной безопасности – совокупность правовых, организационных, и технических мероприятий, средств и норм, направленных на предотвращение или существенное затруднение нанесения ущерба любого характера собственнику и потребителю информации;

Технический канал утечки информации – совокупность объекта разведки, технического средства разведки, с помощью которого добывается информация об объекте, и физической среды, в которой распространяется информационный сигнал;

Техническое обеспечение – комплекс технических средств, предназначенных для работы информационной системы, а также соответствующая документация на эти средства и технологические процессы;

Угроза доступности – угроза нарушения работоспособности информационной системы при доступе к информации;

Угроза конфиденциальности – угроза раскрытия информации;

Угроза целостности – угроза изменения информации;

Угрозы информационной безопасности – совокупность причин, условий и факторов, создающих опасность для объектов информационной безопасности, реализация которых может повлечь нарушение прав, свобод и законных интересов юридических и физических лиц в информационных процессах;

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками;

Ущерб – стоимость потерь, которые понесет сторона в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации. Ущерб зависит только от стоимости информации, которая обрабатывается в информационной системе. Ущерб является характеристикой информационной системы и не зависит от степени ее защищенности;

ISO – Международная организация по стандартизации (International Organization for Standardization, ISO), занимающаяся выпуском стандартов;

IEC – Международная электротехническая комиссия (МЭК; англ. International Electrotechnical Commission, IEC) — международная организация по стандартизации в области электрических, электронных и смежных технологий;

ISO/IEC 17799 – стандарт информационной безопасности, опубликованный в 2005 организациями ISO и IEC. Озаглавлен как «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности» (англ. Information technology – Security techniques – Code of practice for information security management);

Стандарт – в рамках данного документа, под данным термином понимается стандарт информационной безопасности ISO/IEC 17799, если явно неуказанно иное.

Используемые сокращения

ГО	Государственные органы
ИБ	Информационная безопасность
ИС	Информационная система
ИЗ	Информационная защита
НПА	Нормативно-правовой акт
НСД	Несанкционированный доступ
ПИБ	Политика информационной безопасности
ПО	Программное обеспечение
СЗИ	Система защиты информации
СИБ	Служба информационной безопасности
ЭЦП	Электронная цифровая подпись

1. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Главной целью, на достижение которой направлены все положения Политики, является надежное обеспечение информационной безопасности ГП РБ «Бурят-Фармация» и, как следствие, недопущение нанесения материального, физического, морального или иного ущерба в результате проектно-технологической и информационной деятельности.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния:

- доступность обрабатываемой информации для зарегистрированных пользователей;
- устойчивое функционирование ГП РБ «Бурят-Фармация»;
- обеспечения конфиденциальности информации, хранимой, обрабатываемой на средствах вычислительной техники и передаваемой по каналам связи;
- целостность и аутентичность информации, хранимой и обрабатываемой в ГП РБ «Бурят-Фармация» и передаваемой по каналам связи.
- Для достижения поставленной цели необходимо решить следующие задачи:
- защита от вмешательства посторонних лиц в процесс функционирования ГП РБ «Бурят-Фармация»;
- разграничение доступа зарегистрированных пользователей к информации аппаратными, программными и криптографическими средствами защиты, используемыми в ГП РБ «Бурят-Фармация»;
- регистрация действий пользователей при использовании ресурсов ГП РБ «Бурят-Фармация» в системных журналах;
- периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов специалистами информационной безопасности;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защита информации от несанкционированной модификации искажения;
- контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносных кодов, включая компьютерные вирусы;
- обеспечение аутентификации пользователей, участвующих в информационном обмене;
- своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;

- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции;
- создание условий для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабления негативного влияния и ликвидации последствий нарушения безопасности информации.

2. РЕАЛИЗАЦИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Политика информационной безопасности ГП РБ «Бурят-Фармация» является методологической базой:

- выработки и совершенствования комплекса согласованных нормативных, правовых, технологических и организационных мер, направленных на защиту информации;
- обеспечения информационной безопасности;
- координации деятельности структурных подразделений при проведении работ по соблюдению требований обеспечения информационной безопасности.

Для реализации Политики информационной безопасности ГП РБ «Бурят-Фармация» необходимо провести комплекс превентивных мер по защите информации, в том числе конфиденциальных данных, информационных процессов, включающих в себя требования в адрес персонала, менеджеров и технических служб. На основе Политики строится управление информационной безопасностью.

Политика сформирована на основе результатов информационного и технического обследования ГП РБ «Бурят-Фармация» в рамках аудита, результатов анализа информационных рисков и оценки защищенности информации, в соответствии с требованиями нормативно-руководящих документов, а также согласно рекомендациям международных стандартов в области защиты информации.

Политика основана на системном подходе, гарантирующем высокую вероятность достижения тактической цели - снижения неэффективности разрозненных решений, и стратегической цели - реализации возможностей единого системного решения.

3. МЕТОДОЛОГИЯ И ПРИНЦИПЫ ПОСТРОЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ

Целями защиты информации являются: предотвращение утечки, хищения, утраты, искажения, подделки информации, предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в ресурсы ГП РБ «Бурят-Фармация».

В общем контексте безопасность связана с защитой ресурсов от угроз, где угрозы классифицированы на основе потенциала злоупотребления защищаемыми активами.

При разработке политики безопасности использована модель (рис.1) соответствующая международному стандарту ISO/IEC 15408 «Информационная технология – методы защиты – критерии оценки информационной безопасности», стандарту ISO/IEC 17799 «Управление информационной безопасностью».

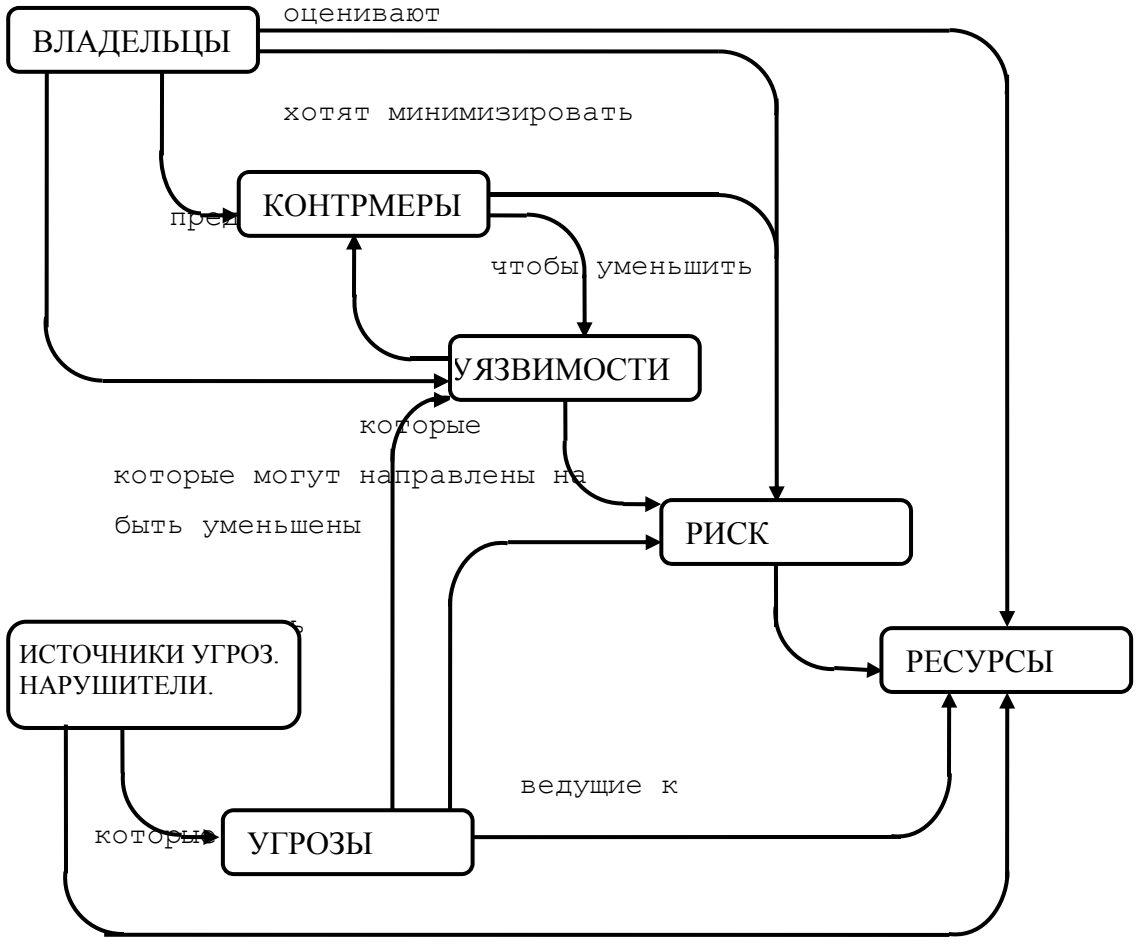

Рисунок 1 – Модель безопасности

Источники угроз – это силы природы, объекты окружающей среды, деструктивные социальные проявления и т. п., которые могут нанести хаотический ущерб ресурсам при возникновении, активизации или изменении своего состояния без стремления к достижению какой-либо цели.

Нарушители – это субъекты и объекты посредством субъектов, которые нанесли ущерб в результате неформализованных действий или бездействия без стремления к достижению какой-либо заранее спланированной цели.

Ресурсы - это данные, создаваемые в процессе функционирования и эксплуатации ПО ГП РБ «Бурят-Фармация», а также программно-аппаратное обеспечение входящие в эксплуатационный комплект.

Контрмеры – предупреждающие действия (решения) принимаемые ГО для предотвращения уязвимости.

Риски - сочетание вероятности наступления уязвимости и его последствий для ресурсов ГП РБ «Бурят-Фармация».

Уязвимость – это потенциальные опасности для функционирования ГП РБ «Бурят-Фармация». В общем случае, уязвимость ассоциируется с нарушением политики безопасности, вызванным неправильно заданным набором правил или ошибкой в обеспечивающей безопасность компьютера программе.

Уязвимость — это состояние системы, которое позволяет:

- исполнять команды от имени другого пользователя;
- получать доступ к информации, закрытой от доступа для данного пользователя;
- показывать себя как иного пользователя или ресурс;

Отдельные категории нарушителей могут быть отнесены к разряду злоумышленников, определяемых как «лицо, которое совершает, или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий». Поскольку такое определение применяется к нарушителю только по решению суда, по понятным причинам далее применяется термин «нарушитель».

Потенциальные нарушители - это субъекты и объекты посредством субъектов, которые могут нанести ущерб в определенных условиях при наступлении определенных событий.

За сохранность рассматриваемых ресурсов отвечают их владельцы, для которых эти ресурсы имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим ресурсам и стремиться использовать их вопреки интересам их

владельца.

Владельцы воспринимают подобные угрозы как потенциал воздействия на ресурсы, приводящего к понижению их ценности для владельца. К специфическим нарушениям безопасности обычно относят (но не обязательно ими ограничиваются): раскрытие ресурса несанкционированным получателем, наносящее ущерб (потеря конфиденциальности); ущерб ресурсу вследствие несанкционированной модификации (потеря целостности) или несанкционированное лишение доступа к ресурсу (потеря доступности).

Владельцы ресурсов анализируют возможные угрозы, чтобы решить, какие из них действительно присущи их среде. В результате анализа определяются риски. Анализ помогает при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня.

Таким образом, ПИБ основывается на модели, которая рассматривает три основных субъекта — владельца, службу информационной безопасности собственника, нарушителя. Владелец передает процессы обеспечения безопасности службе ИБ.

Изначально у службы ИБ отсутствуют знания о нарушителе.

Для построения модели нарушителя в этих условиях используется принцип «черного ящика», действующего как генератор событий, направленных на активизацию угроз через уязвимости, что является достаточным для обеспечения базового уровня безопасности.

В основу разработки и практической реализации ПИБ положены следующие принципы:

1) Невозможность миновать защитные средства;
2) Усиление самого слабого звена;
3) Недопустимость перехода в открытое состояние;
4) Минимизация привилегий;
5) Разделение обязанностей;
6) Многоуровневая защита;
7) Разнообразие защитных средств;
8) Простота и управляемость информационной системы;
9) Обеспечение всеобщей поддержки мер безопасности.

Принцип невозможности миновать защитные средства означает, что все информационные потоки в подсистемы ГП РБ «Бурят-Фармация» и из них должны проходить через СЗИ.

Надежность любой СЗИ определяется самым слабым звеном. Часто таким звеном

оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

Принцип недопустимости перехода в открытое состояние означает, что при любых обстоятельствах (в том числе и нештатных), СЗИ либо полностью выполняет свои функции, либо должна полностью блокировать доступ.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно для предотвращения злонамеренных или неквалифицированных действий системного администратора.

Принцип многоуровневой защиты предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией — управление доступом и, как последний рубеж, — протоколирование и аудит. Эшелонированная оборона способна, по крайней мере, задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками преодоления СЗИ.

Принцип простоты и управляемости информационной системы в целом и СЗИ в особенности определяет возможность формального или неформального доказательства корректности реализации механизмов защиты. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование.

Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Рекомендуется с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

4. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЕСЭДО, МЕТОДЫ И СРЕДСТВА

4.1. Виды угроз

Основными действиями, которые производятся с информацией и могут содержать в себе угрозу, являются сбор, модификация, утечка и уничтожение данных. Эти действия являются базовыми для дальнейшего рассмотрения.

Все источники угроз ГП РБ «Бурят-Фармация» разделяются на внешние и внутренние.

Источниками внутренних угроз являются:

1. сотрудники организации;
2. ПО;
3. аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

1. ошибки пользователей и системных администраторов;
2. нарушения сотрудниками установленных регламентов сбора, обработки, передачи и уничтожения информации;
3. ошибки в работе ПО;
4. отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

1. компьютерные вирусы и вредоносные программы;
2. организации, службы и отдельные лица;
3. стихийные бедствия.

Формами проявления внешних угроз являются:

1. заражение компьютеров вирусами или вредоносными программами;
2. несанкционированный доступ (НСД) к корпоративной информации;
3. информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;
4. действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации;
5. аварии, пожары, техногенные катастрофы.

4.2. Методы и средства информационной безопасности

Обеспечение информационной безопасности ГП РБ «Бурят-Фармация» реализуется следующими формами защиты:

1. правовой;
2. организационной;
3. программно- аппаратной.

4.2.1. Правовые методы обеспечения информационной безопасности

Основой правовой формы обеспечения информационной безопасности являются:

Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации от 07 июля 2003 № 126-ФЗ «О связи»;

Федеральный закон Российской Федерации от 10 января 2002 № 1-ФЗ «Об электронной цифровой подписи»;

Федеральный закон Российской Федерации от 9 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;

Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;

Указ Президента Российской Федерации от 12 мая 2004 г. № 611 «О мерах по обеспечению информационной безопасности российской федерации в сфере международного информационного обмена»;

Постановление Правительства Российской Федерации от 03 ноября 1994 г. №1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Приказ Гостехкомиссии России от 30 августа 2002 г. № 282;

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения;

ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;

ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний;

ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения;

РД 50-682-89. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения;

РД 50-34.698-90. Методические указания. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов;

РД 50-680-89. Методические указания. Автоматизированные системы. Основные положения;

ГОСТ 6.38-72. Система организационно-распорядительной документации. Требования к оформлению;

ГОСТ 6.10-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения;

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;

РД Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей. Утвержден приказом Гостехкомиссии России от 4 июня 1999 г. №114;

РД Средства защиты информации. Специальные общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам. Гостехкомиссия России, 2000 г;

Приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»;

Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена ФСТЭК России 14 февраля 2008 г.);

Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена ФСТЭК России 15 февраля 2008 г.);

Положение о персональных данных;

Положение о разрешительной системе допуска пользователей к конфиденциальной информации и персональным данным;

Положение о постоянно действующей комиссии по защите конфиденциальной информации и персональных данных в ГП РБ «Бурят-Фармация»;

Перечень сведений конфиденциального характера и персональных данных;

План мероприятий по защите конфиденциальной информации и защите персональных данных;

Акт классификации информационных систем персональных данных;

Инструкция по обеспечению информационной безопасности при подключении и

использовании информационно-вычислительной сети общего пользования;

Инструкция пользователя ИСПДн;

Обязанности администратора информационной безопасности;

Журнал учета обращений субъектов ПДн;

Инструкция по действиям персонала во внештатных ситуациях при обработке конфиденциальной информации и персональных данных;

Соглашение работника ГП РБ «Бурят-Фармация» о неразглашении информации, составляющей персональные данные ИСПДн;

Инструкция по организации антивирусной защиты;

Инструкция администратора информационной безопасности;

Инструкция по организации парольной защиты;

Инструкция администратора баз данных;

Инструкция по работе с ключевыми носителями в информационных системах обработки персональных данных;

4.2.2. Организационные формы защиты

Организационной формой защиты являются (но не ограничиваются) мероприятия, предусмотренные данной ПИБ. К ним относятся:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании технической инфраструктуры ГП РБ «Бурят-Фармация» и других ассоциированных с ней объектов;
- мероприятия по разработке правил доступа пользователей к ресурсам системы согласно политике безопасности;
- мероприятия, осуществляемые при подборе и подготовке персонала;
- организацию охраны и режима допуска к системе;
- организацию учета, хранения, использования и уничтожения документов и носителей информации;
- распределение реквизитов разграничения доступа;
- организацию контроля за работой пользователей;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и ПО.

Организационные меры защиты осуществляются и поддерживаются службой информационной безопасности (далее СИБ), которая в обязательном порядке должна быть создана в организации.

Состав, назначение и функции СИБ должны соответствовать действующему законодательству.

Основной задачей СИБ является поддержка уровня ИБ организации на заданном уровне, определение направления развития мер, направленных на защиту информации от несанкционированного доступа, изменения, разрушения или отказа в доступе.

Это достигается путем внедрения соответствующих правил, инструкций и указаний.

СИБ отвечает за:

1. разработку и издание правил (инструкций и указаний) по обеспечению ИБ, соответствующих им правилам работы организации и требованиям к обработке информации;
2. внедрение программы обеспечения ИБ, включая классификацию информации и оценку деятельности;
3. разработку и обеспечение выполнения программы обучения и ознакомления с основами информационной безопасности в масштабах организации;
4. разработку и сопровождение перечня минимальных требований к процедурам контроля над доступом ко всем компьютерным системам, независимо от их масштаба;
5. отбор, внедрение, проверку и эксплуатацию соответствующих методик планирования восстановления работы для всех подразделений организации, принимающих участие в автоматизированной обработке самой важной информации;
6. разработку и внедрение процедур пересмотра правил обеспечения информационной безопасности, а так же рабочих программ, предназначенных для поддержки правил, инструкций, стандартов и указаний организации;
7. участие в описании, конструировании, создании и приобретении систем в целях соблюдения правил безопасности при автоматизации производственных процессов;
8. изучение, оценку, выбор и внедрение аппаратных и программных средств, функций и методик обеспечения информационной безопасности, применимых для компьютерных систем организации.

При необходимости на СИБ возлагается выполнение других обязанностей:

1. участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
2. распределение между пользователями необходимых реквизитов защиты;
3. наблюдение за функционированием системы защиты и ее элементов;
4. организация проверок надежности функционирования системы защиты;
5. обучение пользователей и персонала ИС правилам безопасной обработки информации;
6. контроль за соблюдением пользователями и персоналом ИС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;
7. принятие мер при попытках НСД к информации и при нарушениях правил функционирования системы защиты.

Организационно-правовой статус службы:

1. численность службы защиты должна быть достаточной для выполнения всех перечисленных функций;
2. подчиненность СИБ определяется структурой организации;
3. сотрудники СИБ должны иметь право доступа во все помещения, где установлена аппаратура ИС и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;
4. руководителю СИБ должно быть предоставлено право запрещать включение в число действующих новые элементы ИС, если они не отвечают требованиям ИБ;
5. СИБ должна иметь все условия, необходимые для выполнения своих функций.

4.2.3.1.Физическая безопасность

Критическое или чувствительное оборудование обработки информации должно быть размещено в охраняемых зонах, защищено определенными периметрами безопасности, оснащенными соответствующими барьерами безопасности и средствами контроля на входе. Они должны быть физически защищены от несанкционированного доступа, повреждения или создания помех в работе.

Применительно к безопасности окружающей среды должны быть разработаны (и применяться) меры по физической защите от ущерба в результате пожаров, наводнений, землетрясений, взрывов, массового гражданского неповиновения, а также от других видов бедствий естественного или искусственного характера.

Обеспечиваемая защищенность должна быть пропорциональна идентифицированным

рискам.

Физическая безопасность реализуется совокупностью способов защиты на основе инженерных конструкций в сочетании с техническими средствами охраны, образующих физическую защиту. Составной частью физической защиты - является инженерная защита и техническая охрана объектов (ИЗТОО).

Требуемый уровень информационной безопасности достигается многозональностью и многорубежностью защиты, которая должна быть обеспечена с помощью инженерной защиты и охраны системы.

Организационно – технологическая среда представляет собой единый комплекс информационных и технических ресурсов, эксплуатирующего и обслуживающего персонала.

4.2.3.1.Требования к рабочему месту пользователя (администратора)

В состав типового рабочего места входят:

1) компьютер (комплект – системный блок, монитор, клавиатура, манипулятор «мышь», многогнездная розетка-удлинитель (опция), источник бесперебойного питания (опция));

2) мебель рабочего места (стол письменный (канцелярский), стул, тумбочка…).

В целях обеспечения требований физической безопасности компьютер как комплект должен быть проверен на информационную безопасность и соответствующим образом сертифицирован и опломбирован. В случае обнаружения факта, изменения состава комплекта или нарушения пломбы сертификат считается отозванным, дальнейшее использование компьютера прекращается и может быть возобновлено только по результатам сертификации или заключения экспертной комиссии.

Должно быть минимизировано количество путей доступа к ресурсам компьютера, удалить (физически отключить) «лишние», неиспользуемые для повседневной штатной работы порты (COM, USB, RS,…), флоппи и CD/DVD дисководы.

Монитор следует располагать таким образом, чтобы исключить возможность просмотра содержимого экрана посторонними лицами, в том числе извне с помощью оптических приборов.

Особое внимание следует уделять условиям хранения носителей с резервными копиями ресурсов, а также ключей физической защиты (Aladdin, eToken и т.д.). Они должны храниться в запираемом и опечатываемом металлическом сейфе или тубусе. Должен быть обеспечен быстрый доступ к носителю в условиях чрезвычайной ситуации.

Не следует загромождать поверхность рабочего стола не используемыми в данный

момент документами, носителями, а также оставлять их на столе при уходе с рабочего места на продолжительное (например, более 2 часов) время. Следует соблюдать режим «чистого стола» - ничего лишнего, только самое необходимое на данный момент работы.

Аналогичные правила должны распространяться и на «рабочий стол» монитора. Не следует держать открытыми большое число «окон» или сбрасывать их в строку состояния. Должен использоваться паролируемый хранитель экрана.

В качестве носителей информации должны использоваться носители, полученные пользователем непосредственно в организации. Каждый носитель должен иметь заводской номер изготовителя, маркерную метку или не снимаемую этикетку с маркерной меткой организации, датой ввода в эксплуатацию и инвентарным номером ресурса в системе ИБ, соответствующему номеру в карточке ресурса. Использование носителей, не отвечающих этим требованиям, категорически запрещается.

Для хранения носителей с оперативными резервными копиями данных и состояния системы должны быть определены место и средства хранения и соблюдены условия хранения применительно к типу конкретного носителя.

Поскольку состав рабочего места администраторов в целом соответствует вышеприведенному, аналогичные требования и рекомендации распространяются также и на рабочие места администраторов.

4.2.3.2.Требования к серверному оборудованию и серверному помещению

Требования к серверу как к единице оборудования в отношении ИБ в целом соответствуют требованиям, предъявляемым оборудованию системы.

Общие требования к серверному помещению должны отвечать требованиям, приведенным в технической документации изготовителя или стандарте EIA/TIA 569.

Стойка (шкаф) сервера должны быть закрыты со всех сторон стенками и запираться на ключ (если это предусмотрено конструкцией). Не должно быть понятий «зимнего» и «летнего» режима, когда сервер эксплуатируется со снятыми стенками.

В зависимости от конструктивных особенностей, сервер может поставляться как в виде комплектного моноустройства, так и в виде отдельных блоков, предназначенных для монтажа в аппаратную стойку или шкаф, в том числе и открытого исполнения, что приводит к ликвидации одного рубежа защиты, поскольку невозможно устранить неконтролируемый физический доступ к элементам сервера, также существенно усложняется и сертификация. В этом случае ужесточаются требования к серверному помещению в части контроля доступа, которые должны компенсировать ликвидацию одного рубежа защиты. Должны быть обязательно предусмотрены: металлическая дверь с

замком повышенной секретности, система контроля доступа с выводом сигнала тревоги на ПЦО, система видеонаблюдения. Физический доступ персонала в серверное помещение должен осуществляться согласно указаниям п. 9.1.2 стандарта ISO 17799.

Особое внимание следует уделять физическому порядку в серверном помещении. Категорически запрещается использовать серверное помещение для складирования посторонних предметов. Необходимо составить перечень оборудования из состава сервера и задействованных обеспечивающих систем (UPS, автономный кондиционер и т.д.), нахождение которого обоснованно необходимо в серверном помещении, указать ответственного за поддержание порядка. Перечень в распечатанном виде должен быть помещен на видное место.

В целях обеспечения работоспособности, возможности производительной эксплуатации в течение всего срока службы оборудования необходимо выполнять комплекс ремонтно-профилактических мероприятий, предусмотренный технической документацией. С этой целью составляется план таких работ в рамках внутри- и межремонтных циклов с указанием вида, даты начала и планируемого окончания работ.

При производстве всех видов ремонтно-профилактических работ должны быть предусмотрены меры по недопущению реализации угрозы типа «отказ в доступе». С этой целью рекомендуется до начала выполнения работ предусмотреть возможность перехода на резервный режим и проверить готовность такого перехода.

4.2.3.3.Разделения сред разработки, тестирования и рабочей среды.

В целях уменьшения рисков несанкционированного доступа или изменения системы рабочее оборудование должно быть отделено от оборудования, на котором производится разработка и тестирование.

Должен быть определен и реализован необходимый уровень разделения сред разработки, тестирования и рабочей среды.

Должны быть определены и документированы правила передачи ПО из стадии разработки в стадии тестирования, полноценного рабочего использования.

Разрабатываемое (тестируемое) и рабочее ПО должны использоваться на различных системах и располагаться в различных доменах или каталогах

Системные утилиты не должны быть доступны из операционных систем, когда это не требуется;

При определении уровня разделения рабочей среды и среды тестирования должны учитываться следующие требования:

среда системы, на которой выполняется тестирование, должна быть как можно более

близкой к среде рабочей системы;

для уменьшения рисков ошибок пользователи должны использовать различные пользовательские профили в рабочей системе и в системе для тестирования. Меню на обеих системах должны отображать соответственно одинаковые идентификационные сообщения;

тестирование должно выполняться на наборе данных, некритичных для ИБ.

Для выполнения этих требований для целей тестирования и отладки ПО должен использоваться отдельный тестовый стенд.

4.2.3.4.Управление услугами, предоставляемыми третьими сторонами

В целях осуществления и поддержания соответствующего уровня информационной безопасности при использовании услуг, предоставляемых третьей стороной, организация должна проверять наличие в договорных обязательствах соглашений требований по вопросам ИБ, осуществлять мониторинг соответствия соглашений и управлять изменениями, гарантирующими, что предоставляемые услуги удовлетворяют всем требованиям соглашения с третьей стороной.

4.2.3.5.Транспортировка физических носителей информации

Носители, содержащие информацию, должны быть защищены от несанкционированного доступа, неправильного использования или повреждения при транспортировке вне физических границ организации.

Рекомендации по реализации

Должны быть рассмотрены следующие рекомендации по защите носителей информации, транспортируемых между территориями:

следует использовать надежных курьеров или надежный транспорт;

с руководством организации должен быть согласован список уполномоченных курьеров;

должны быть разработаны процедуры проверки личности курьеров;

упаковка должна обеспечивать достаточную защиту контента от любого физического повреждения, которое, вероятнее всего, может возникнуть при транспортировке;

она должна соответствовать спецификациям любых производителей;

упаковка должна обеспечивать защиту от любых факторов окружающей среды, которые могут уменьшить эффективность восстановления данных с носителей информации, например, из-за нагревания, влажности или электромагнитных полей;

при необходимости должны применяться средства управления, защищающие чувствительную информацию от несанкционированного раскрытия или изменения; можно привести следующие примеры:

использование запираемых контейнеров;

доставка вручную;

запечатанная упаковка (обеспечивающая обнаружение попыток вскрытия);

в исключительных ситуациях - разбиение всего отправляемого груза на несколько партий и отправка их к пункту назначения по различным маршрутам.

4.2.3.6.Программные и аппаратные формы защиты

Программными и аппаратными формами защиты являются (но не ограничиваются) мероприятия, предусмотренные данной ПИБ. К ним относятся:

идентификацию и аутентификацию пользователей;

разграничение доступа к ресурсам;

регистрацию событий;

криптографические преобразования;

проверку целостности системы;

проверку отсутствия вредоносных программ;

программную защиту передаваемой информации и каналов связи;

защиту системы от наличия и появления нежелательной информации;

создание физических препятствий на путях проникновения нарушителей;

мониторинг и сигнализацию соблюдения правильности работы системы;

создание резервных копий информации.

4.2.3.7.Защита электронного обмена данными

Информация, передаваемая в виде электронных сообщений, должна быть соответствующим образом защищена. ИБ ГП РБ «Бурят-Фармация» в целом зависит и от состояния ИБ при обмене сообщениями в других системах, функционирующих на тех же технических средствах, что и ГП РБ «Бурят-Фармация». При рассмотрении безопасности электронного обмена данными в этих системах необходимо учитывать следующее:

1) должна быть предусмотрена защита сообщений от несанкционированного доступа, изменения или отказа в обслуживании;
2) должна быть обеспечена правильная адресация и транспортировка сообщения;
3) должна быть обеспечена надежность и доступность обслуживания;
4) должны быть учтены требования законодательства, в частности, требования,

предъявляемые к ЭД и ЭЦП;

5) должно быть предусмотрено использование более строгих правил идентификации при доступе из сетей общего пользования и обеспечен контроль их соблюдения.

Для уменьшения риска, которому подвергаются производственные процессы и система безопасности, связанного с использованием электронной почты, следует применять (по необходимости) соответствующие средства контроля. Необходимо учитывать:

1) уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;
2) уязвимость данных, пересылаемых по электронной почте, по отношению к ошибкам, например, неправильная адресация или направление сообщений не по назначению, а также надежность и доступность сервиса в целом;
3) влияние изменения характеристик коммуникационной среды на производственные процессы, например, влияние повышенной скорости передачи данных или изменения системы адресации между организациями и отдельными лицами;
4) правовые соображения, такие, как необходимость проверки источника сообщений и др.;
5) последствия для системы безопасности от раскрытия содержания каталогов;
6) необходимость принятия защитных мер для контроля удаленного доступа пользователей к электронной почте.

Организации должны задать четкие правила, касающиеся статуса и использования электронной почты.

4.2.3.8.Защита от злонамеренного и мобильного кода

С целью защиты информации и программных средств от несанкционированного доступа и действия вредоносных программ) при разработке и эксплуатации системы должны быть предприняты организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий. При этом руководство должно обеспечить неукоснительное выполнение следующих мероприятий:

Сертификация - действия третьей стороны, цель которых - подтвердить (с помощью сертификата соответствия) то, что изделие (в том числе программное средство) или услуга, прямо или косвенно взаимодействующая с системой, соответствует определенным стандартам или другим нормативным документам в области защиты информации.

Профилактика - систематические действия эксплуатационного персонала, цель

которых - выявить и устранить неблагоприятные изменения в свойствах и характеристиках используемых программных средств, в частности проверить эксплуатируемые, хранимые и (или) вновь полученные программные средства на наличие компьютерных вирусов.

Ревизия - проверка вновь полученных программ специальными средствами, проводимая путем их запуска в контролируемой среде.

Вакцинирование - обработка файлов, дисков, каталогов, проводимая с применением специальных программ, создающих условия, подобные тем, которые создаются определенным компьютерным вирусом, и затрудняющих повторное его появление.

4.2.3.9.Средства управления для борьбы со злонамеренными программными кодами

В качестве мер для борьбы со злонамеренными программными кодами должны быть реализованы средства управления для предотвращения его ввода, его обнаружения и восстановления системы после удаления злонамеренного программного кода, а также поддержания компетентности пользователей в этой области.

При этом учитываются следующие рекомендации:

1. необходимо внедрить правила, запрещающие использование нелегального ПО;
2. должны быть внедрены формальные правила защиты от рисков, связанных с получением файлов и ПО из внешней сети или на любом другом носителе;
3. необходимо проводить регулярные проверки ПО и баз данных систем, поддерживающих критические производственные процессы; должно формально исследоваться наличие любых подозрительных файлов или несанкционированных исправлений;
4. должны быть обеспечены:
    a. установка и регулярное обновление ПО для обнаружения злонамеренного кода и восстановления среды после его удаления (пакеты антивирусных программ и библиотеки к ним),
    b. сканирование содержимого компьютеров и носителей информации в виде профилактического или регулярно выполняемого средства управления, обеспечивающего:
    c. проверку на злонамеренные коды перед использованием любых полученных файлов - на внешних носителях, полученных по сетям;
    d. проверку прикрепленных файлов электронной почты и загруженных файлов на злонамеренные коды перед их использованием. Эта проверка должна выполняться на различных участках, например, на серверах электронной

почты, настольных компьютерах, на входе в сеть организации;

5. определение процедур управления и обязанностей, связанных с защитой систем от злонамеренного кода, обучение их использованию, уведомлению о злонамеренных кодах, восстановлению среды после атак, предпринятых злонамеренным кодом;
6. подготовка соответствующих планов непрерывного ведения бизнеса, предусматривающих восстановление среды после атак, обусловленных злонамеренным кодом, в том числе все необходимые данные и ПО для копирования и мер по восстановлению;
7. реализация процедур проверки информации, касающейся злонамеренного кода, гарантирование того, что бюллетени с предупреждениями точны и информативны; руководители должны гарантировать, что для того, чтобы отличить мистификации от реальных злонамеренных кодов будут использоваться квалифицированные источники, например, журналы, имеющие хорошую репутацию, надежные сайты в сети Интернет или поставщики защитного ПО; все пользователи должны быть оповещены о проблемах, связанных с мистификациями и о том, что следует делать при получении мистифицированного злонамеренного кода.

С целью повышения эффективности защиты от злонамеренных кодов необходимо предусмотреть использование в среде обработки информации двух или более программных продуктов – «антивирусов» различных поставщиков.

В установленном, для защиты от злонамеренных кодов, ПО необходимо обеспечить поддержку автоматического обновления файлов определения и утилит сканирования, что гарантирует своевременное обновление защиты.

Кроме того, это ПО может быть установлено на каждом рабочем месте для выполнения автоматических проверок.

Должны быть приняты меры предосторожности по защите от ввода злонамеренных кодов во время обслуживания и процедур работы при чрезвычайных обстоятельствах, при которых могут игнорироваться традиционно используемые средства управления защитой от злонамеренных кодов.

5. ПЕРЕСМОТР ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Соблюдение требований Политики информационной безопасности обязательно для всех категорий сотрудников эксплуатирующих и пользующихся ИСПДн ГП РБ «Бурят-Фармация». Проведение планового аудита информационной безопасности является одним из основных методов проверки эффективности мер по защите информации. Результаты аудита могут служить основанием для пересмотра некоторых положений Политики и внесения в них необходимых корректировок.

Целесообразно ежегодно проводить аудит информационной безопасности ИСПДн ГП РБ «Бурят-Фармация», и должен проводиться пересмотр Политики на предмет соответствия предъявляемым требованиям. В случае возникновения необходимости, при выявлении в процессе аудита несоответствия современным требованиям вносить изменения и дополнения.

Кроме этого, используемые информационные технологии и организация служебной деятельности непрерывно меняются, это приводит к необходимости корректировать существующие подходы к обеспечению информационной безопасности.