УТВЕРЖДАЮ:

ДИРЕКТОР ФБУ ЦЕНТР
РЕАБИЛИТАЦИИ ФОНДА
СОЦИАЛЬНОГО СТРАХОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
«ТОПАЗ»

_____
М.Л. ЗЕВАКИН

«10» _____ 2012 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.Назначение

Политика информационной безопасности ФБУ ЦЕНТР РЕАБИЛИТАЦИИ ФОНДА СОЦИАЛЬНОГО СТРАХОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ «ТОПАЗ» (далее Учреждение) является основополагающим документом, определяющим систему приоритетов, принципов и методов достижения целей обеспечения защищенности информационных активов Учреждения.

Целью настоящей Политики является защита интересов Учреждения и его стабильности путем определения процесса обеспечения информационной безопасности, соответствующего потребностям и обязательствам Учреждения.

Политика исходит из того, что обеспечение информационной безопасности Учреждения как системно-значимой представляет собой комплексную многоуровневую и многоаспектную задачу, включающую различные объекты и цели защиты, характер угроз, способы противодействия им, а также критерии оценки эффективности систем безопасности.

2.Общие положения

2.1. Область применения

Политика является обязательной к применению в Учреждении. Выполнение требований политики является обязательным для всех сотрудников Учреждения.

Политика также распространяется на все деловые, договорные, финансовые, информационные, публичные или иные взаимодействия Учреждения с третьими лицами или Учреждениями, которые прямо или косвенно могут влиять на информационную безопасность Учреждения.

Настоящая Политика является руководящим документом для следующих групп сотрудников Учреждения:

- Руководство Учреждения;
- Конечные пользователи АРМ;
- Обладатели информационных активов;
- Операторы информационных систем;
- Группа автоматизированной системы управления.

Положения настоящей Политики должны применяться при определении наиболее важных объектов защиты, формулировке принципов и направлений работ по разработке необходимых мер защиты информационных активов, сопровождения, обслуживания и

обеспечения нормального функционирования корпоративной информационной системы Учреждения, а также при ручной или автоматизированной обработке и хранении информации, содержащей сведения, составляющие коммерческую, служебную тайну, персональные или иные, подлежащие защите, критичные данные ограниченного доступа.

2.2. Нормативные ссылки

В настоящей Политике использованы ссылки на следующие нормативные документы:

- Закон РФ от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Закон РФ от 21 июля 1993 г. № 5485-1 "О государственной тайне";
- Закон РФ от 29 июля 2004 г. № 98-ФЗ "О коммерческой тайне";
- Закон РФ от 27 июля 2006 г. № 152-ФЗ "О персональных данных";
- Международный стандарт ISO/IEC 17799:2005 «Информационные технологии – Методы обеспечения безопасности – Практические правила управления информационной безопасностью»;
- Международный стандарт ISO/IEC 27001:2005 «Информационные технологии - Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования»;
- ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»;
- ГОСТ 28906-91 «Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель»;
- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
- COBIT 4.1 – The Control Objectives for Information and related Technology;
- Толковый словарь современной информационно-правовой лексики, под редакцией Леонова А.П., 2002 г.;
- Перечень информации, составляющий коммерческую тайну Учреждения;

2.3 Термины, определения и сокращения

Термины и определения, используемые в данной Политике, определены с использованием ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» и Толкового словаря современной информационно-правовой лексики, под редакцией Леонова А.П., 2002 г.

Также для целей настоящего Положения в нем определены следующие термины, определения и сокращения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Анализ риска – систематическое использование информации для идентификации источников риска и оценки риска.

Аудит информационной безопасности – систематический процесс получения и оценки данных о текущем состоянии информационной безопасности информационных активов Организации, устанавливающий соответствие определенным критериям и предоставляющий результаты Руководству Организации.

Доступность – свойство информации и связанных с ней активов быть доступной для авторизованных пользователей по мере необходимости.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная технология – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

Информационная безопасность Учреждения – механизм защиты, обеспечивающий конфиденциальность, целостность и доступность информации, обращающейся в учреждении.

Информационные активы Учреждения – информация, в том числе содержащаяся в информационных системах учреждения, представляющая ценность для учреждения с точки зрения достижения его интересов (целей).

Инцидент информационной безопасности – единичное нежелательное или неожиданное событие (или серия нежелательных или неожиданных событий) в системе информационной безопасности, которые приводят или с определенной вероятностью могут привести к компрометации информационных активов или иному ущербу информационной безопасности.

Катастрофоустойчивость – способность информационной системы сохранять работоспособность в условиях деградации ее архитектуры, вызванной массовым уничтожением ее элементов и взаимосвязей между ними в результате масштабных природных, техногенных катастроф или террористических актов.

Криптографическая защита информации – защита конфиденциальности информации путем использования средств шифрования.

Конфиденциальность – свойство информации быть доступной только для авторизованных пользователей.

Мониторинг информационной безопасности – оперативное и постоянное наблюдение за объектами, являющимися объектами информационной безопасности, а также объектами, влияющими на обеспечение информационной безопасности, проведение сбора, анализа и обобщения результатов наблюдения в соответствии с заданными целями.

Несанкционированный доступ к информационным активам – доступ к информации, нарушающий установленные правила разграничения доступа.

Обладатель информационного актива – сотрудник или подразделение Учреждения, которое уполномочено Руководством Учреждения исполнять по отношению к информационному активу административные обязанности: учет, категорирование, управление развитием, обслуживанием, использованием, обеспечением безопасности и координация деятельности в этих направлениях. Термин «обладатель» не означает, что сотрудник или подразделение действительно имеет какие-либо права собственности на сам актив.

Объект информационной безопасности – защищаемые Учреждением информация, носитель информации или процесс.

Оператор информационной системы – сотрудник или подразделение Учреждения, которое уполномочено осуществлять деятельность по эксплуатации информационных систем, в том числе по обработке информации, содержащейся в её базах данных

Оценивание риска – процесс оценки угроз, их последствий, уязвимости информации и средств ее обработки, а также вероятности их возникновения.

Риск – это вероятность возникновения события, которое окажет отрицательное воздействие на достижение целей Учреждения.

Риск-аппетит – это степень риска, которую Учреждение считает для себя приемлемой в процессе достижения своих целей.

Система информационной безопасности (СИБ) – взаимоувязанный комплекс организационных, нормативно-правовых мер и аппаратно-программных комплексов и средств, обеспечивающих защиту от возникновения случайных и преднамеренных инцидентов информационной безопасности.

Система скоординированной деятельности по руководству и управлению информационной безопасностью центра реабилитации «Топаз» (СУИБ) – часть общей корпоративной деятельности по руководству и управлению «Топаз», предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения его информационной безопасности. Система общей корпоративной деятельности по руководству и управлению центра реабилитации «Топаз» включает структуру, политики, деятельности по планированию, обязанности, практики, процедуры, процессы и ресурсы центра реабилитации «Топаз». (Данное определение соответствует ISO/IEC IS 27001).

Уровень защиты информации – перечень обязательных к выполнению требований по защите информации, обеспечивающий необходимую величину остаточного риска.

Управление рисками информационной безопасности – процесс выявления, контроля и минимизации или устранения рисков информационной безопасности, оказывающих влияние на информационные системы, в рамках допустимых затрат.

Целостность – свойство достоверности и полноты информации

АРМ – автоматизированное рабочее место.

ИБ – информационная безопасность.

ИС – информационная система.

КИС – корпоративная информационная система.

КСИБ – комплексная система информационной безопасности.

ЛВС – локально-вычислительная сеть.

ПО – программное обеспечение.

ПЭВМ – персональная электронно-вычислительная машина.

СИБ – система информационной безопасности.

СУИБ – Система управления информационной безопасностью.

3.Общие направления политики информационной безопасности

3.1. Общие положения

Информационная безопасность Учреждения строится, прежде всего, учитывая требования Российского законодательства, а так же ориентируясь на стандарты в области информационной безопасности – ISO/IEC IS 27001:2005 и ISO/IEC IS 17799:2005 и ГОСТ Р ИСО/МЭК 17799-2005. Выбор данных стандартов обусловлен тем, что рекомендации, изложенные в них, являются гибкими и универсальными. Описанный в выбранных стандартах набор лучших практик применим практически к любой организации, независимо от формы собственности, вида деятельности, размера и внешних условий. Выбранные стандарты нейтральны в технологическом плане, и всегда существует возможность выбора технологий, удовлетворяющих требованиям Учреждения.

3.2. Рекомендации международных стандартов

Учреждение следует рекомендациям международных стандартов в сфере информационной безопасности, направленным на:

• Проведение регулярного анализа возможных причин и последствий нарушения принципов непрерывности (анализа рисков);

• Учет величины возможного ущерба от реализации рисков нарушения информационной безопасности при планировании затрат на обеспечение информационной безопасности, т.е. на минимизацию рисков;

• Снижение возможного ущерба, вызванного актами терроризма, катастрофами, стихийными бедствиями и неблагоприятными природными явлениями, отказами элементов систем обеспечения безопасности;

• Снижение зависимости от монопольных поставщиков программных, технических средств, расходных материалов и услуг;

• Разработку и реализацию планов действий на случай чрезвычайных обстоятельств для обеспечения гарантий того, что процессы могут быть восстановлены в пределах приемлемого времени для надлежащего выполнения соответствующих функций;

• Обеспечение наличия всех необходимых средств для уменьшения рисков, ограничение последствий разрушительных воздействий и своевременное возобновление деятельности.

Обеспечение информационной безопасности Учреждения включает осознание необходимости информационной безопасности и важности процессов управления ИБ.

Осознание необходимости ИБ относится как к Руководству Учреждения, так и к сотрудникам на всех звеньях системы управления ИБ, вплоть до рядовых исполнителей.

Задачи обеспечения ИБ определяют ответственность сотрудников Учреждения в части реализации принципов обеспечения ИБ, определенных настоящей Политикой, а также требований раздела 5 «Ответственность высшего Руководства организации» международного стандарта ISO/IEC IS 27001:2005.

3.3.Организация управления информационной безопасностью

Процесс управления информационной безопасностью Учреждения является комплексным и включает выполнение ряда функций на различных уровнях управления:

• Учет, классификация и контроль информационных активов;
• Разработка требований по ИБ к КИС Учреждения;
• Планирование, развитие и сопровождение СИБ;
• Создание и поддержание в актуальном состоянии нормативно-методической базы ИБ;
• Обеспечение информационной безопасности от угроз, связанных с персоналом;
• Мониторинг состояния информационной безопасности Учреждения;
• Управление рисками ИБ;
• Управление инцидентами ИБ;
• Совершенствование СУИБ;
• Управление непрерывностью процессов деятельности;
• Решение организационных вопросов безопасности;
• Физическая защита и защита от воздействий окружающей среды;
• Контроль выполнения требований ИБ при передаче данных и операционной деятельности;
• Управление контролем доступа;
• Контроль выполнения требований ИБ при разработке и обслуживании информационных систем;
• Контроль обеспечения соответствия ИБ требованиям законодательства РФ, нормативно-технических и руководящих документов по ИБ в РФ и Учреждение.

3.4.Стратегия обеспечения информационной безопасности

Стратегия обеспечения информационной безопасности Учреждения заключается в планировании, развертывании, эксплуатации и совершенствовании системы управления информационной безопасностью, адекватно отвечающей потребностям Учреждения. СУИБ должна обеспечивать достижение целей деятельности Организации в условиях:

• Штатного функционирования;
• Возникновения локальных инцидентов и проблем информационной безопасности;
• Возникновения широкомасштабных катастроф и аварий различной природы, последствия которых имеют или могут иметь отношение к эффективной работе Учреждения в целом.

При построении СУИБ Учреждение ставит своей задачей соответствовать уровню не ниже 4 модели зрелости процесса DS5 «Обеспечение безопасности систем» в соответствии с «Целями контроля для информационных и смежных технологий – стандарта COBIT 4.1» (Приложение 1).

3.5.Комплекс мер для обеспечения информационной безопасности

Информационная безопасность Учреждения обеспечивается на основе согласованного комплекса организационных, нормативно-правовых мер и программно-технических средств, включающих:

- Контроль за соблюдением юридических норм, определяющих взаимоотношения с внешними организациями;
- Контроль за соблюдением соглашений с внешними организациями и физическими лицами о конфиденциальности или неразглашении, отражающие потребности Учреждения и подвергающиеся регулярному пересмотру;
- Построение организационной структуры Учреждения, устанавливающей задачи, ответственность и подчиненность подразделений в ИБ;
- Планирование, разработку, согласование, ввод в действие и контроль за выполнением внутренних нормативных документов Учреждения, устанавливающих обязанности и ответственность персонала за нарушения информационной безопасности;
- Применение технических и программных средств защиты;
- Контроль за выполнением организационно-технических норм и регламентов, определяющих стадии жизненного цикла информационных систем Учреждения, включающих технические и программные средства защиты (создание, ввод в действие, эксплуатация, модернизация и вывод из эксплуатации);
- Обучение и переподготовку специалистов по ИБ. Вопросы обеспечения ИБ должны решаться сотрудниками, обладающими необходимым уровнем знаний;
- Проведение обязательного обучения персонала основам информационной безопасности, обеспечение регулярных переподготовок и контроля знаний;
- Мониторинг, внутренний контроль и аудит подсистем информационной безопасности (включенных в состав ИС), а также возникающих угроз с целью минимизации рисков.

Информационная безопасность Учреждения обеспечивается в условиях централизованно-распределённой структуры средств защиты информационных активов Учреждения с учётом возможности воздействия следующих условий и факторов:

- Подверженность катастрофам, действиям террористов и иных внешних злоумышленников;
- Зависимость от внешних поставщиков аппаратно-программных средств, расходных материалов, телекоммуникационных услуг и т.п.;
- Невозможность обработки информации в связи с отказом технических средств;
- Неправильное (нарушающее установленный регламент) администрирование аппаратно-программных и технических средств;
- Неправильное (нарушающее установленный регламент) управление информационными активами;
- Ошибочные или злонамеренные действия персонала.

Учреждение финансирует мероприятия, связанные с решением задач по информационной безопасности, исходя из результатов оценки рисков и выбора адекватных мер по их снижению, в объемах и в сроки, обеспечивающие достижение следующих целей:

- Обеспечение приемлемого уровня защищенности информационных активов Организации, т.е. риск нарушения конфиденциальности, доступности и целостности информационных активов Учреждения соответствует риск-аппетиту Учреждения;
- Соответствие уровню не ниже 4 модели зрелости процесса DS5 «Обеспечение безопасности систем» в соответствии с «Целями контроля для информационных и смежных технологий – COBIT 4.1» (Приложение 1).

3.6. Защищаемые объекты информационной безопасности

Учреждение защищает от угроз, связанных с рисками информационной безопасности, следующие типы объектов:

- Информационные активы (информацию) Учреждения;
- Программное обеспечение (целостность компонентов ПО информационных систем);
- Физические устройства, хранящие, обрабатывающие и передающие информацию;
- Бизнес-процессы (услуги).

3.7. Основные угрозы информационной безопасности

Подробный перечень угроз информационной безопасности определяется на этапе анализа рисков. Основываясь на практиках, изложенных в отечественных и международных стандартах, Учреждение выделяет основные угрозы защищаемых ресурсов:

3.7.1. Внешние угрозы

- Атаки из внешних информационных сред на аппаратно-программные и технические комплексы и информационные активы Организации, в том числе компьютерные вирусы;
- Катастрофы и неблагоприятные события природного и техногенного характера;
- Террористические акты;
- Зависимость от монопольных поставщиков аппаратно-программных и технических средств, расходных материалов, услуг и т.п.

3.7.2. Внутренние угрозы

- Невыполнение (или неполное выполнение) сотрудниками Учреждения и привлеченным персоналом, в т.ч. консультантами и специалистами фирм, привлекаемых в рамках аутсорсинга, установленных технических и/или технологических регламентов;
- Несанкционированная деятельность (включая ошибки) персонала и пользователей информационных систем, приводящая к уменьшению уровня защищенности, т.е. снижению количества (или изменению состава) выполненных требований по защите информационных систем, необходимого для отнесения данных систем к тому или иному классу защищенности информационных систем;
- Нецелевое использование информационных активов, средств вычислительной техники и сетей передачи данных Учреждения;
- Несанкционированный доступ к информационным активам (чтение, копирование, публикация, искажение, частичное или полное уничтожение, ввод ложной информации и т.п.);
- Сбои, отказы.

3.8. Подходы к формированию основных требований обеспечения информационной безопасности

Требования обеспечения информационной безопасности в Учреждение формируются на основе анализа рисков информационной безопасности, характерных для ресурсов Учреждения. Для достижения целей обеспечения информационной безопасности Учреждения, в условиях отсутствия методологии проведения анализа рисков, требования формируются на основе экспертных оценок специалистов, ответственных за обеспечение ИБ в Учреждении, согласованных с подразделениями ИТ.

Корректировка требований обеспечения информационной безопасности при необходимости должна производиться на основании анализа действий по выполнению

требований ИБ и оценки остаточных (после выполнения требований) рисков информационной безопасности.

4.Направления реализации политики информационной безопасности в автоматизированных системах

4.1.Определение защищаемых информационных активов Учреждения

Точный перечень информационных активов, попадающих в область действия СУИБ, должен быть определен на этапе инвентаризации информационных активов. Организация выделяет следующий перечень видов информационных систем и входящих в них информационных активов, являющихся наиболее приоритетными с точки зрения обеспечения их информационной безопасности:

- системы, хранящие, обрабатывающие и передающие информацию, охраняемую согласно законодательству РФ или иным документам, содержащим обязательные для выполнения Учреждения требования по защите информации (информация, составляющая коммерческую, служебную тайну, персональные данные) или иные, критичные для бизнеса, сведения;
- системы автоматизации делопроизводства и документооборота.

К перечисленным системам применимы как общие принципы обеспечения информационной безопасности, так и специфические для каждого вида принципы, меры и средства защиты.

В автоматизированных информационных системах Учреждения присутствует информация, различная с точки зрения необходимости и уровня обеспечения её защиты. Каждому виду информации соответствуют свои приоритеты обеспечения целостности, конфиденциальности и доступности.

Приоритеты в организации защиты информации, являющейся собственностью государства или защита которой регламентируется государством, определяются с учетом положений соответствующих государственных нормативно-методических документов. Приоритеты в организации защиты иной информации определяются обладателями данной информации, исходя из её ценности (значимости) для Организации и его клиентов.

4.2 Информация, хранящаяся, обрабатывающаяся и передающаяся в информационных системах Организации.

4.2.1 Общедоступная информация

Общедоступная информация, предназначенная для официальной передачи во внешние организации, средства массовой информации и т.п., а также информация, полученная из внешних открытых источников.

4.2.2 Информация ограниченного доступа

Информация ограниченного доступа делится на три категории:

1) сведения, относящиеся к государственной тайне: режим устанавливается уполномоченным государственным органом на основании закона РФ от 21 июля 1993 г. N 5485-1 "О государственной тайне" (в рамках КИС Организации данная информация не обрабатывается);

2) конфиденциальная информация (в том числе информация, составляющая коммерческую тайну Учреждения или третьих лиц). Режим защиты информации Организации устанавливается на основании Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и Федерального закона от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне" (с действующими изменениями);

3) персональные данные. Режим защиты информации устанавливается специальным Федеральным законом N 152-ФЗ от 27 июля 2006 года "О персональных данных".

4.3 Ответственность Учреждения

Учреждение несет ответственность за:

- достоверность информации, официально предоставляемой им внешним организациям и гражданам;
- достоверность и выполнение регламента предоставления внешним организациям информации, обязательность и порядок предоставления которой определены законодательством Российской Федерации и/или нормативными документами Учреждения и/или закреплены в договорах (соглашениях);
- обеспечение соответствующего законодательству Российской Федерации, заключенным договорам (соглашениям) и внутренним нормативным документам уровня защиты, как собственной информации, так и информации, переданной Учреждению официально внешними организациями и гражданами.

4.4. Общие требования по информационной безопасности к информационным системам Учреждения

В информационных системах Учреждения должны быть выполнены следующие требования информационной безопасности:

- Каждая информационная система Учреждения должна обеспечивать предоставление каждому пользователю системы, к которой он получил легитимный доступ, индивидуальный, уникальный идентификатор;
- Для каждой учетной записи в ИС должен быть определен сотрудник или группа сотрудников, несущих ответственность за её использование;
- Каждая информационная система Учреждения должна иметь возможность обеспечить предоставление каждому пользователю минимальных прав, достаточных для исполнения им своих функциональных обязанностей;
- Каждая ИС должна иметь встроенные механизмы безопасности и должна быть настроена в соответствии с требованиями к настройкам информационной безопасности информационных систем;
- Каждая ИС должна иметь средства регистрации изменений функциональности информационных систем, мониторинга пользовательской активности, особенно активности привилегированных учетных записей, а также контроль прав доступа к инструменту аудита пользовательской активности;
- К каждой информационной системе Учреждения должен предоставляться доступ пользователя к информационному активу Учреждения на основании заявки, утвержденной директором в установленном порядке;
- Для каждой информационной системы Учреждения должна быть обеспечена защита от доступа пользователя в базы данных в обход прикладного клиентского ПО;
- Для каждой информационной системы Учреждения должна быть обеспечена защита от действий в явном виде не разрешенных пользователю и запрещенных ему по умолчанию.

В случае если в некоторых подсистемах или для некоторых групп пользователей информационных систем Учреждения выдвигаются дополнительные требования по защите информации, такие подсистемы (группы пользователей) объединяются в выделенные сегменты с применением сертифицированных средств, позволяющих реализовать указанные дополнительные требования (межсетевые экраны и т.п.).

Доступ пользователей Учреждения к сети Интернет возможен в режиме межсетевого экрана на базе UserGate 5 . Организация доступа и порядок использования информации, полученной из сети Интернет, регулируется «Инструкцией по использованию сети Интернет».

Доступ для всех подразделений Учреждения, подключенных к КИС Учреждения, предоставляется через единый шлюз, принадлежащий Учреждению и находящийся в его

управлении. На указанном шлюзе реализуется безопасная развязка между внутренними сетями Учреждения и сетью Интернет. На шлюзе также реализуется подсистема регистрации и автоматизированного анализа действий пользователей, а также обеспечивается анализ и контроль информационных потоков. Объем и порядок реализации функций анализа и контроля определяет администратор сети.

Обновление программного обеспечения ИС из сети Интернет должно осуществляться только с использованием специализированных защищенных шлюзов или серверов обновлений.

4.5. Основные требования по ИБ при эксплуатации информационных систем

- Порядок допустимого использования информационных активов, средств вычислительной техники и сетей передачи данных;
- Порядок установки и модификации программного, аппаратного и информационного обеспечения;
- Порядок настройки и администрирования элементов информационных систем (серверов, активного оборудования и т.д.);
- Предоставление доступа сотрудникам Учреждения к информационным активам Учреждения;
- Предоставление доступа к информационным активам Учреждения персонала третьей стороны, оказывающего услуги по поддержке и эксплуатации ресурсов Организации;
- Права и обязанности персонала при работе с информационными активами Учреждения;
- Права и обязанности персонала при работе с ресурсами сети Интернет;
- Порядок работы со съемными носителями и устройствами записи;
- Порядок работы с паролями;
- Порядок обнаружения несанкционированной активности;
- Порядок обнаружения вредоносного программного обеспечения.

5.Сферы ответственности при реализации политики информационной безопасности.

5.1. Ответственность Руководства Учреждения

Руководство обязано активно поддерживать информационную безопасность Учреждения путем явной установки целей безопасности информации, назначения и контроля исполнения обязанностей персонала в области информационной безопасности.

В сферу ответственности Руководства Учреждения входит:

- Управление процессом обеспечения информационной безопасности в Учреждение;
- Рассмотрение и поддержка инициатив в области информационной безопасности;
- Контроль того, что цели информационной безопасности:
  - определены;
  - установлены;
  - соответствуют требованиям законодательства, обязательным для Учреждения нормативно-техническим документам, а также обеспечения бизнеса;
  - интегрированы в процессы Учреждения;
- Выделение необходимых ресурсов для обеспечения деятельности в области информационной безопасности.

5.2. Ответственность конечных пользователей

В сферу ответственности конечных пользователей АРМ входят:

- Соблюдение установленных в Учреждении Политик, правил и процедур обработки и хранения информации;

- Работа в информационных системах в соответствии с действующими Политиками, требованиями безопасности к конкретным системам и приложениям, соответствующими инструкциями и другой внутренней нормативной и организационно-распорядительной документацией;
- Информирование Руководства и администраторов систем о неправомерных действиях других пользователей, нарушающих установленные правила информационной безопасности.

6.Ответственность за нарушения положений Политики

Сотрудники Учреждения, нарушившие положения настоящей Политики, несут административную, материальную и/или дисциплинарную ответственность в соответствии с действующим законодательством и/или условиями трудового соглашения вплоть до увольнения по инициативе Руководства. В отдельных случаях возможно привлечение сотрудников Учреждения к уголовной ответственности в установленном законом порядке.

Приложение 1

МОДЕЛЬ ЗРЕЛОСТИ

Процесса DS5 «ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ»

(в соответствии со сборником методик и рекомендаций – COBIT 4.1)

Модель управления информационной безопасностью (ИБ) определяет шесть уровней зрелости организации — с нулевого по пятый.

Нулевой уровень ("несуществующий")

Организация не осознаёт необходимость в обеспечении безопасности ИТ. Не определена ответственность и подотчётность по вопросам обеспечения безопасности. Не реализованы меры управления безопасности ИТ. Не предусмотрены процедуры информирования по состоянию безопасности ИТ и реагирования на случаи нарушения безопасности. Полностью отсутствует какой-либо процесс управления обеспечением безопасности.

Первый уровень ("начальный")

Организация осознаёт необходимость в обеспечении безопасности ИТ. Однако степень этого осознания зависит от конкретных сотрудников. Меры по обеспечению безопасности ИТ, фактически, являются лишь реакцией на происходящие события и никак не оцениваются. Не определена ответственность при обнаружении случаев нарушения безопасности ИТ. Реакции на случаи нарушения безопасности непредсказуемы.

Второй уровень ("повторяемый")

Ответственным и подотчётным лицом по вопросам обеспечения безопасности ИТ назначен координатор по вопросам обеспечения безопасности ИТ, не получивший при этом никаких управленческих полномочий. Знания по вопросам обеспечения безопасности имеют фрагментарный и ограниченный характер. Хотя информация, имеющая отношение к вопросам безопасности, генерируется системами, она не анализируется. Услуги сторонних организаций могут не отвечать специфическим потребностям организации. Разработаны политики безопасности, однако, продолжают использоваться неадекватные методы и средства. Отчётность по вопросам обеспечения безопасности страдает неполнотой, может ввести в заблуждение и быть бесполезной. Обучение по вопросам безопасности доступно, однако проводится в основном по инициативе отдельных сотрудников. Обеспечение ИТ безопасности понимается , в первую очередь, как обязанность службы ИТ и корпоративное руководство не принимает участие в управлении ИТ безопасностью.

Третий уровень ("определенный")

Имеется осведомлённость по вопросам обеспечения безопасности, её повышение поощряется руководством. Определены процедуры обеспечения безопасности ИТ, соответствующие политике безопасности. Назначены лица, ответственные за обеспечение безопасности, однако их деятельность не в полной мере внедрена в практику. Существует план по обеспечению безопасности ИТ, обеспечивающий проведение анализа рисков. Отчётность по вопросам безопасности не в полной мере сосредоточена на потребностях бизнеса. Эпизодически выполняется тестирование аспектов обеспечения безопасности (например, возможности взлома системы).

Четвертый уровень ("управляемый")

Чётко определены и внедрены ответственности по управлению ИТ безопасностью. Последовательно выполняется анализ рисков ИТ безопасности, а также возможных последствий. Завершено создание политик и процедур обеспечения безопасности, определены основные направления обеспечения безопасности с учётом особенностей данной организации. Информирование по вопросам осведомлённости и безопасности носит обязательный характер. Стандартизованы идентификация, аутентификация и авторизация пользователей. Введена аттестация персонала, ответственного за аудит и

управление безопасностью. Тестирование системы безопасности является стандартизованным и формализованным процессом, направленным на повышение безопасности. Процессы обеспечения безопасности ИТ координируются со службой общей безопасности всей организации. Отчётность по обеспечению безопасности ИТ увязана с целями бизнеса. Обучение по вопросам обеспечения безопасности проводится как для бизнес - подразделений, так и для персонала ИТ. Это обучение планируется и осуществляется в соответствии с бизнес- потребностями и выявленными рисками безопасности . Цели и показатели управления безопасностью определены, но пока не подвергаются оценке.

Пятый уровень ("оптимизированный")

Руководители основных бизнес-подразделений и ИТ службы несут солидарную ответственность по вопросам обеспечения безопасности ИТ, которые интегрированы с корпоративными целями обеспечения безопасности бизнеса. Требования по обеспечению безопасности ИТ чётко определены, оптимизированы и включены в утверждённый план мероприятий по обеспечению безопасности. Конечные пользователи и потребители ИТ услуг всё в большей степени отвечают за определение требований по безопасности, а функции обеспечения безопасности интегрированы с прикладными задачами на стадии проектирования. В случае инцидентов немедленно применяются формализованные и автоматизированные процедуры реагирования. В ходе периодически проводимых оценок состояния безопасности проверяется эффективность выполнения плана мероприятий по обеспечению безопасности. Систематически собирается и анализируется информация о новых угрозах и уязвимых местах. Своевременно обсуждаются и принимаются меры по снижению уровня опасности. Тестирование аспектов безопасности, анализ основных причин случаев нарушения безопасности и заблаговременное выявление рисков – всё это служит основой непрерывного повышения уровня безопасности. Процессы и технологии обеспечения безопасности интегрированы в рамках организации. Фиксируются, собираются и доводятся до сведения заинтересованных сторон показатели управления безопасностью. Руководство применяет эти данные для постоянного совершенствования плана обеспечения безопасности.