ПОЛИТИКА ООО «ТЦИ» В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1 О ПОЛИТИКЕ

В рамках осуществления деятельности, связанной с обслуживанием Главного реестра и системы регистрации национальных доменов .RU, .РФ и домена .SU, Общество с ограниченной ответственностью «Технический Центр Интернет» (далее – Общество) считает важнейшей задачей обеспечение защиты информационных активов Общества, аккредитованных регистраторов, партнеров и контрагентов.

Для решения этой задачи в Обществе применяется система управления информационной безопасностью в соответствии с принципами и требованиями международного стандарта «ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems –Requirements».

2 ЦЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Система управления информационной безопасности способствует реализации миссии и бизнес-целей Общества, а также достижению целей и выполнению задач подразделений. Основными целями информационной безопасности являются:

- обеспечение конфиденциальности, целостности и доступности информационных активов;

- обеспечение прозрачности процессов информационной безопасности;

- выполнение требований ICANN и IANA в области информационной безопасности;

- минимизация рисков информационной безопасности при ведении операционной деятельности Общества;

- обеспечение непрерывности основной деятельности Общества;

- выполнение нормативно-правовых требований к обеспечению информационной безопасности;

- повышение деловой репутации и корпоративной культуры.

3 ПРИНЦИПЫ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

С целью обеспечения эффективности системы управления информационной безопасностью Общество руководствуется следующими фундаментальными принципами:

- вовлеченность высшего руководства в процессы управления информационной безопасностью;

Деятельность по обеспечению информационной безопасности осуществляется по инициативе и под контролем высшего руководства Общества. Для проведения регулярного анализа со стороны руководства и принятия решений по совершенствованию системы управления информационной безопасностью в Обществе действует комитет по информационной безопасности, возглавляемый Генеральным директором. Общая координация деятельности по обеспечению информационной безопасности осуществляется Начальником отдела информационной безопасности.

- законность обеспечения информационной безопасности;

Меры обеспечения информационной безопасности выбираются в соответствии с международными стандартами, законодательством Российской Федерации и нормативными документами ФСТЭК России и ФСБ России.

- риск-ориентированный подход к управлению информационной безопасностью;

Меры обеспечения информационной безопасности активов выбираются на основании оценки рисков информационной безопасности, которая учитывает вероятность реализации угроз информационной безопасности и величину возможного ущерба от их реализации, а также устанавливает приемлемые уровни риска.

- квалификация персонала;

Персонал проходит строгий и тщательный отбор, вырабатывается и поддерживается корпоративная этика, что создает благоприятную среду для деятельности и снижает риски информационной безопасности.

- управление инцидентами информационной безопасности;

Общество постоянно выявляет, учитывает и оперативно реагирует на действительные, предпринимаемые и вероятные нарушения информационной безопасности, а также принимает меры по предотвращению повторения подобных нарушений. Реагирование на инциденты осуществляется в режиме 24x7.

- стремление к постоянному совершенствованию системы управления информационной безопасностью;

Общество постоянно повышает эффективность системы управления информационной безопасности, выполняя требования политик, обеспечивая достижение целей информационной безопасности, реализуя корректирующие и предупреждающие действия по результатам независимых внутренних и

внешних аудитов, анализа событий и инцидентов информационной безопасности, анализа со стороны высшего руководства.

- повышение осведомленности в сфере информационной безопасности;

Требования в области информационной безопасности доводятся до сведения персонала и контрагентов в части их касающейся. Персонал проходит регулярное обучение и повышение осведомленности по вопросам информационной безопасности.

- дисциплинарная ответственность;

Работники Общества несут персональную ответственность за нарушение требований информационной безопасности. Обязанности по обеспечению информационной безопасности включаются в трудовые договоры и должностные инструкции

работников, а также в договоры (соглашения) с контрагентами.

- учет действий с информационными активами;

Постоянно ведется учет всех действий персонала и контрагентов с информационными активами Общества.

- предоставление минимально необходимых прав доступа;

Персоналу и контрагентам предоставляются права доступа, минимально необходимые для качественного и своевременного выполнения трудовых обязанностей и договорных обязательств.

4 ОБНАРУЖЕНИЕ АТАК «УНИЧТОЖЕНИЕ/БЛОКИРОВАНИЕ ДОСТУПА К ИНФОРМАЦИИ» И ПРОТИВОДЕЙСТВИЕ ИМ

Атака «уничтожение/блокирование доступа к информации» – воздействие на информационный актив (сервис) Общества, приводящий сервис в состояние, при котором пользователи сервиса не могут получить доступ к информации, либо этот доступ затруднён.

Общество обеспечивает обнаружение и предотвращение как внешних, так и внутренних атак, направленных на уничтожение и/или блокирование доступа к информации Общества. Общество использует системы обнаружения и системы снижения эффективности таких атак. Применяются системы мониторинга, настроенные на обнаружение ситуаций с блокированием доступа к информации.

Общество приветствует направление в свой адрес уведомлений о недоступности информационных систем Общества от аккредитованных регистраторов и от владельцев информационных активов (сервисов).

Общество имеет право применять защитные и/или ограничительные меры в отношении участника информационного взаимодействия в случае, если деятельность участника информационного взаимодействия угрожает стабильности, безопасности, надежности и непрерывности функционирования информационных систем и бизнес-процессов Общества.

При обнаружении атаки «уничтожение/блокирование доступа к информации», направленной на общедоступный информационный актив (сервис) Общества защитные и/или ограничительные меры применяются незамедлительно. При этом если между Обществом и участником существуют договорные отношения с указанием контактных данных, подходящих для экстренного уведомления (адрес электронной почты), участнику будет выслано уведомление в обязательном порядке. Если обнаружена атака на ресурсы общества со стороны третьих лиц – защитные и/или ограничительные меры предпринимаются без предварительного уведомления.

Договоры на оказание услуг Обществом, где в состав услуг входит доступ к информационным активам Общества, содержат информацию о мерах, которые Общество имеет право применять в случае, если деятельность участника информационного взаимодействия угрожает стабильности, безопасности, надежности и непрерывности функционирования информационных систем и бизнес-процессов Общества.