



Технический
Центр
Интернет

Политика АО «Технический Центр Интернет» в области информационной безопасности

Политика

На 6 страницах

Информация о документе

Индекс документа

Статус документа

Дата начала действия документа

Версия

Дата окончания действия документа

П

Технические нормы

06.03.2017

2.4

1 О Политике

В рамках осуществления деятельности, связанной с обслуживанием Главного реестра и системы регистрации национальных доменов .RU, .РФ и домена .SU, АО «Технический Центр Интернет» 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 Политике АО «Технический Центра Интернет» в области информационной безопасности 4 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.
- риско-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 Политика АО «Технический Центра Интернет» в области информационной безопасности 5 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.

Приложение 1. Список внесенных изменений

История изменения документа

Дата изменения	Номер версии	Описание изменения
30.09.2016	2.2	Обновлен уровень поддерживаемого стандарта безопасности до версии ISO/IEC 27001:2013.
24.01.2017	2.3	Документ дополнен описанием мер выявления и противодействия для атак «уничтожение/блокирование доступа к информации» (см. раздел 4).
06.03.2017	2.4	Доработан раздел 4. Уточнен порядок уведомлений о принятых мерах против выявленной атаки.

Контакты АО «Технический центр Интернет»

- Адрес: 127083, Москва, улица 8 Марта, дом 1 строение 12.
- Телефон: +7 (495) 730-29-69.

Клиентская служба

Клиентская служба Технического центра Интернет:

- Телефон: +7 (495) 730-29-69.