

Приложение

УТВЕРЖДЕНА

постановлением администрации
муниципального образования
Северский муниципальный район
Краснодарского края
от _____ № _____

ПОЛИТИКА аудита информационной безопасности администрации муниципального образования Северский район Краснодарского края

1. Общие положения

1.1. Настоящая Политика аудита информационной безопасности администрации муниципального образования Северский муниципальный район Краснодарского края (далее – Политика) определяет единый системный подход к осуществлению контроля обеспечения информационной безопасности администрации муниципального образования Северский муниципальный район Краснодарского края (далее - администрация) посредством проведения аудита информационной безопасности.

1.2. Настоящая Политика разработана в соответствии с:
приказом Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

методическим документом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.3. Аудит информационной безопасности проводится с целью:
анализа рисков, связанных с возможностью осуществления угроз безопасности в отношении защищаемой информации;
оценки текущего уровня защищённости информационных систем;
выявления и локализации «слабых» мест в системе защиты информации администрации;

оценки соответствия информационных систем требованиям регулирующих органов и внутренним нормативным документам, регламентирующим процессы обработки и защиты информации в администрации;

выработки рекомендаций по внедрению новых и повышению эффективности существующих механизмов обеспечения безопасности защищаемой информации.

1.4. Аудит информационной безопасности может проводиться:

самостоятельно работниками администрации, ответственными за обеспечение защиты информации – внутренний аудит;

на договорной основе со сторонними организациями, имеющими лицензию Федеральной службы по техническому и экспортному контролю Российской Федерации (далее — ФСТЭК России) на деятельность по технической защите конфиденциальной информации, в соответствии с постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» – внешний аудит.

2. Внутренний аудит информационной безопасности

2.1. Внутренний аудит заключается в оценке выполнения требований нормативных документов по обеспечению безопасности и защищённости информации, обрабатываемой администрацией.

2.2. Внутренний аудит представляет собой непрерывную и неотъемлемую часть деятельности, по обеспечению информационной безопасности администрации, осуществляемой на следующих этапах жизненного цикла информационных систем:

на предпроектном этапе;

на этапе проектирования;

на этапе подготовки к вводу в эксплуатацию;

на этапе проведения опытных испытаний;

на этапе эксплуатации.

2.3. Внутренний аудит должен проводиться:

с использованием сертифицированных ФСТЭК России автоматизированных средств контроля (анализа) защищённости и соответствия требованиям – инструментальный аудит;

без использования автоматизированных средств – аналитический аудит.

2.4. Внутренний аудит может быть плановый: ежегодный, проводимый с целью проверки степени выполнения администрацией требований по обеспечению информационной безопасности, так и периодический, проводимый в отношении структурных подразделений администрации (форма планов проведения внутреннего аудита представлена в приложении 1 к настоящей Политике), а также внеплановый.

2.5. Внеплановый внутренний аудит может проводиться в случае:

наличия косвенных подтвержденных сведений о нарушениях работниками администрации требований к обеспечению информационной безопасности;

многократных инцидентов нарушения информационной безопасности, случившихся в структурных подразделениях администрации;

подготовки к контролю со стороны уполномоченных федеральных органов, регулирующих деятельность в сфере обработки и защиты информации.

2.6. Внеплановый внутренний инструментальный аудит может проводиться после появления информации об уязвимости и соответствующем обновлении баз средств контроля (анализа) защищённости.

2.7. Внутренний аналитический аудит проводится в целях проверки:

- назначения лиц, ответственных за защиту информации;

- определения соответствия состава и структуры программно-технических средств, обрабатывающих защищаемую информацию (в том числе средств защиты информации), документированному составу и структуре средств, разрешённых для обработки такой информации;

- соответствия реального уровня полномочий по доступу к информационным ресурсам (системам), внутренним документам;

- правильности применения средств защиты информации;

- организации хранения носителей информации и допуска в помещения, в которых размещены средства обработки информации и осуществляется обработка защищаемой информации;

- выполнения требований к условиям размещения технических средств, обрабатывающих защищаемую информацию, в служебных помещениях;

- выполнения требований, предъявляемых к порядку обработки и защиты персональных данных;

- проверки знания работников администрации требований руководящих документов, технологических инструкций, предписаний, актов, заключений и уровень овладения технологией безопасной обработки информации, описанной в этих документах.

2.8. Структура Плана проведения внутреннего аналитического аудита приведена в приложении 2.

2.9. Для проведения внутреннего аналитического аудита информационной безопасности, привлекается комиссия администрации по обеспечению информационной безопасности (далее – комиссия администрации по ОИБ), назначаемая главой муниципального образования Северский район Краснодарского края (далее - глава).

2.10. Члены комиссии администрации по ОИБ имеют право:

- осматривать помещения, в которых производится обработка конфиденциальной информации;

- получать доступ к техническим средствам, участвующим в обработке информации;

- просматривать настройки средств защиты информации;

- проводить беседы и консультации с работниками администрации, требовать от них предоставления письменных объяснений, справок, отчётов по вопросам, относящимся к предмету аудита.

2.11. По результатам внутреннего аналитического аудита:

- комиссией администрации по ОИБ в двухнедельный срок составляется акт о результатах внутреннего аудита администрации, выявленных

недостатках и нарушениях, а также разрабатывается план устранения выявленных в ходе проведения внутреннего аналитического аудита информационной безопасности недостатков (далее - План) (форма Плана приведена в приложении 3), который передается на согласование главе администрации;

глава администрации, при необходимости, вносит изменения в данный План и контролирует реализацию его пунктов;

лица, назначенные ответственными за реализацию пунктов Плана, в согласованный срок отчитываются о результатах проделанной работы.

2.12. Внутренний инструментальный аудит проводится в целях:

выявления (поиска) уязвимостей, связанных с ошибками кода в программном обеспечении средств защиты информации, с правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также с корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

контроля, установленного на АРМ и серверах информационных систем программного обеспечения и соответствие его Реестру разрешённого к использованию в информационных системах Администрации программного обеспечения;

контроля установки обновлений программного обеспечения;

проверки выполнения требований, установленных организационно-распорядительными документами администрации, регламентирующими процессы обработки и защиты информации.

наблюдения за действиями пользователей информационных систем с целью контроля соблюдения ими норм и требований обеспечения безопасности информации, установленных в администрации;

получения актуальных и объективных данных о текущем состоянии обеспечения безопасности информационных систем (в том числе от внешних угроз со стороны потенциальных злоумышленников);

контроля возникновения и устранения уязвимостей и ошибок конфигурации информационных систем;

оценки и отражения в отчётах текущего уровня защищённости информационных ресурсов (систем), средств обработки информации, динамики его изменения;

разработки рекомендаций по повышению уровня безопасности информационных ресурсов (систем), средств обработки информации.

2.13. Периодичность проведения инструментального аудита напрямую зависит от критичности информационных ресурсов (систем), средств обработки информации и составляет:

для информационных ресурсов (систем), средств обработки информации с высокой критичностью – раз в 2 недели;

для информационных ресурсов (систем), средств обработки информации со средней критичностью – ежемесячно;

для информационных ресурсов (систем), средств обработки информации с низкой критичностью – раз в 1 – 3 месяца.

2.14. Сканирование информационных ресурсов (систем), средств обработки информации, в процессе которого выявляются уязвимости программного обеспечения, рекомендуется совмещать со сканированием, в процессе которого анализируются параметры безопасности ресурсов (систем), средств обработки информации.

2.15. Внутренний инструментальный аудит проводится администратором информационной безопасности. При проведении аудита им могут привлекаться иные лица, ответственные за отдельные информационные ресурсы (системы), средства обработки информации.

2.16. По результатам внутреннего инструментального аудита администратором информационной безопасности разрабатывается отчет с описанием выявленных уязвимостей и планом мероприятий по их устранению и принятия последующих мер, направленных на устранение выявленных уязвимостей.

2.17. Выявленные в ходе сканирования информационных ресурсов (систем), средств обработки информации уязвимости и несоответствия следует классифицировать по уровню связанных с ними рисков согласно следующей методологии:

№ п/п	Уровень риска	Возможности и ограничения нарушителя при эксплуатации уязвимости	Срок устранения уязвимости
1	2	3	4
1	Наивысший уровень	Эксплуатация уязвимости/несоответствия позволяет нарушителю установить полный контроль над информационным ресурсом (системой), средством обработки информации в целом или развернутым на нем приложением	7 дней
2	Высокий уровень	Эксплуатация уязвимости/несоответствия позволяет нарушителю получить несанкционированный доступ к защищаемой информации или сервису	14 дней
3		Эксплуатация уязвимости/несоответствия позволяет нарушителю установить полный контроль над информационным ресурсом (системой), средством обработки информации в целом или развернутым на нем приложением. Эксплуатация возможна только при определенных условиях, например, при особой конфигурации информационных ресурсов (систем), средств обработки информации	14 дней

1	2	3	4
4	Средний уровень	Эксплуатация уязвимости/несоответствия нарушителем приводит к отказу в обслуживании информационных ресурсов (систем), средств обработки информации	30 дней
5		Эксплуатация уязвимости/несоответствия позволяет нарушителю повысить свои привилегии и получить несанкционированный доступ к защищаемой информации или сервису, контроль над информационным ресурсом (системой), средством обработки информации или развернутым на нем приложением. Для эксплуатации уязвимости/несоответствия нарушителю требуется удалённый доступ к информационному ресурсу (системе), средству обработки информации с определёнными привилегиями	30 дней
6	Низкий уровень	Эксплуатация уязвимости/несоответствия позволяет нарушителю повысить свои привилегии без получения несанкционированного доступа к защищаемой информации или сервису. Для эксплуатации уязвимости/несоответствия нарушителю требуется санкционированный доступ к данному информационному ресурсу (системе), средству обработки информации	45 дней
7		Эксплуатация уязвимости/несоответствия предоставляет нарушителю чувствительную информацию, полезную для развития атаки	45 дней
8	Нулевой уровень	Эксплуатация уязвимости/несоответствия предоставляет нарушителю общедоступную информацию об информационном ресурсе (системе), средстве обработки информации	60 дней
9		Эксплуатация уязвимости/несоответствия позволяет нарушителю повысить свои привилегии без получения несанкционированного доступа к защищаемой информации или сервису. Для эксплуатации уязвимости/несоответствия	60 дней

1	2	3	4
		нарушительно требуется локальный доступ к информационному ресурсу (системе), средству обработки информации	

2.18. Основной характеристикой уязвимости (несоответствия), на основании которой принимается решение о её устранении или отказе от устранения, является присваиваемый ей приоритет. Приоритет оценивается администратором информационной безопасности на основании уровня риска, связанного с уязвимостью, и уровня критичности информационного ресурса (системы), средства обработки информации. Рекомендуемый критерий определения приоритета приведён ниже¹⁾:

Уровень риска	Уровень критичности информационного ресурса (системы), средства обработки информации		
1	2		
	Высокий	Средний	Низкий
Наивысший	Высокий	Высокий	Средний
Высокий	Высокий	Средний	Низкий
Средний	Высокий	Средний	Низкий
Низкий	Средний	Низкий	Низкий
Нулевой	Низкий	Низкий	Низкий

2.19. Устранение выявленных уязвимостей информационных ресурсов (систем), средств обработки информации осуществляется ответственным за данный информационный ресурс (систему) и средство обработки информации или администратором информационной безопасности. Устранение выявленных уязвимостей должно осуществляться, в том числе, путём установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств или применения комплекса компенсирующих мер (например, дополнительная настройка средств защиты информации; изменение режима и порядка использования информационного ресурса (системы), средства обработки информации).

2.20. В ходе внутреннего аудита в проверяемых структурных подразделениях должна быть получена объективная и полная информация по состоянию обеспечения информационной безопасности.

2.21. Внутренний аудит отдельного структурного подразделения и (или) сегмента информационной инфраструктуры считается окончательным

¹⁾ Критерий не является строгим, и администратор информационной безопасности может увеличивать или уменьшать (имея на это обоснование) приоритет уязвимости (несоответствия) с учётом особенностей информационного ресурса (системы), средства обработки информации и характера уязвимости

после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

2.22. Каждое полугодие комиссией администрации по ОИБ на основании сведений, полученных в ходе проведения аудитов информационной безопасности, разрабатываются рекомендации, в которых отражаются необходимые корректирующие воздействия, направленные на совершенствование процессов обеспечения информационной безопасности (анализ причин возникновения выявленных недостатков и предложения по исключению подобных недостатков в будущем), предложения по корректировке организационно-распорядительной документации, регламентирующей процессы обработки и защиты информации (в том числе Моделей угроз безопасности информации).

3. Внешний аудит информационной безопасности

3.1. Внешний (экспертный) аудит проводится в целях оценки соответствия эффективности применяемых мер защиты установленным требованиям законодательства Российской Федерации и (или) выявления недостатков в системе защиты информации.

3.2. Внешний аудит может проводиться в виде:
тестирования информационной системы на проникновение;
аттестации информационной системы по требованиям безопасности информации.

3.3. Тестирование информационных систем на проникновение, в данном случае, должно осуществляться в режимах «чёрного» или «серого» ящика. Необходимость проведения тестирования на проникновения определяется администратором информационной безопасности.

3.4. Аттестация информационных систем должна проводиться не реже чем раз в три года. Аттестация информационных систем должна проводиться в соответствии с требованиями, утверждёнными национальными стандартами ГОСТ РО 0043-003-2012 и ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».

4. Анализ уязвимостей информационных систем

4.1. Анализ уязвимостей информационных систем, приводящих к возникновению угроз безопасности информации (в том числе на предмет наличия уязвимостей, содержащихся в базе данных угроз ФСТЭК России, располагающейся в сети Интернет по адресу <http://bdu.fstec.ru>) должен обязательно проводиться при:

проектировании системы защиты информации информационной системы;

внедрении системы защиты информации информационной системы;

аттестации информационной системы на соответствие требованиям безопасности информации.

4.2. Анализ уязвимостей может проводиться как при проведении внутреннего инструментального аудита информационной безопасности, так и при внешнем тестировании информационной системы на проникновение.

5. Ответственность за исполнение положений настоящей Политики

5.1. Администратор информационной безопасности несёт ответственность за:

- инициацию проведения аудитов информационной безопасности (внутренних и внешних), в том числе с целью анализа уязвимостей информационных систем;

- согласование планов устранения, выявленных в ходе проведения внутреннего аналитического аудита информационной безопасности недостатков;

- обновление базы признаков уязвимостей средства анализа защищённости из достоверных источников;

- проведение внутреннего инструментального аудита информационной безопасности;

- разработку отчётов и рекомендаций (планов) по устранению выявленных уязвимостей информационных ресурсов (систем), средств обработки информации;

- разработку (каждое полугодие) рекомендаций по осуществлению корректирующих воздействий;

- участие в составе комиссии администрации по ОИБ по внутреннему аналитическому аудиту информационной безопасности и разработке (каждое полугодие) рекомендаций по осуществлению корректирующих воздействий;

- обеспечение содействия сторонним организациям, проводящим аттестацию информационных систем по требованиям безопасности информации.

5.2. Администратор информационных систем несет ответственность за:

- устранение уязвимостей, выявленных в ходе проведения внутреннего инструментального аудита;

- обеспечение содействия членам комиссии администрации по ОИБ в ходе проведения аудита, а также сторонним организациям, проводящим аттестацию информационных систем по требованиям к безопасности информации.

5.3. Пользователи информационных ресурсов (систем) несут ответственность за обеспечение содействия членам комиссии администрации по ОИБ в ходе проведения аудита, а также сторонним организациям, проводящим аттестацию информационных систем по требованиям к безопасности информации.

5.4. Лица, виновные в нарушении положений настоящей политики, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой и административной ответственности.

Начальник управления информатизации и
информационной безопасности

Н.Н.Сергиевская