МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ РЕСПУБЛИКИ АЛТАЙ (Минцифра РА)

АЛТАЙ РЕСПУБЛИКАНЫҢ ЦИФРОВОЙ ӦЗҮМИНИҢ МИНИСТЕРСТВОЗЫ (АР Минцифразы)

ПРИКАЗ **JАКАРУ**

«29» декабря 2021 года № 1294

г. Горно-Алтайск

Об осуществлении контроля состояния системы защиты государственных информационных систем Республики Алтай и информационно-телекоммуникационной инфраструктуры исполнительных органов государственной власти Республики Алтай на 2022 год

В соответствии с абзацами вторым и четвертым пункта 4 решения расширенного заседания Совета по информационной безопасности при Главе Республики Алтай, Председателе Правительства Республики Алтай от 22 октября 2021 года, на основании Положения о Министерстве цифрового развития Республики Алтай, утвержденного постановлением Правительства Республики Алтай от 12 декабря 2019 года № 350,

п р и к а з ы в а ю :

1. Утвердить:

методические рекомендации оценки состояния системы защиты государственных информационных систем Республики Алтай и информационно-телекоммуникационной инфраструктуры исполнительных органов государственной власти Республики Алтай на 2022 год (далее – Методические рекомендации), согласно приложению № 1 к настоящему Приказу;

план проведения контроля состояния систем защиты государственных информационных систем Республики Алтай и информационно-телекоммуникационной инфраструктуры исполнительных органов государственной власти Республики Алтай на 2022 год (далее соответственно – План, контроль), согласно приложению № 2 к настоящему Приказу.

2. Отделу по развитию информационных технологий обеспечить:

проведение контроля согласно Плану и Методическим рекомендациям;

сформировать и предоставить отчет по итогам проведенного контроля на заседание Совета по информационной безопасности при Главе Республике Алтай Председателе Правительства Республики Алтай.

3. Контроль за исполнением настоящего Приказа возложить на заместителя министра Алымова С.П.

Исполняющий обязанности
министра В.Г. Челтугашев

Приложение № 2
к приказу Министерства цифрового
развития Республики Алтай
от «29» декабря 2021 г. № 1294

План проведения контроля состояния систем защиты государственных информационных систем Республики Алтай и информационно-телекоммуникационной инфраструктуры исполнительных органов государственной власти Республики Алтай на 2022 год

№ п/п	Исполнительный орган государственной власти Республики Алтай	Вид контроля	сроки проведения контроля
1	Министерство экономического развития Республики Алтай	выездная проверка	16 мая 2022г.- 20 мая 2022г.
2	Министерство финансов Республики Алтай	выездная проверка	23 мая 2022г.- 27 мая 2022г.
3	Министерство образования и науки Республики Алтай	выездная проверка	30 мая 2022г.- 3 июня 2022г.
4	Министерство здравоохранения Республики Алтай	выездная проверка	6 июня 2022г.- 10 июня 2022г.
5	Министерство труда, социального развития и занятости населения Республики Алтай	выездная проверка	13 июня 2022г. - 17 июня 2022г.
6	Министерство культуры Республики Алтай	выездная проверка	20 июня 2022г. – 24 июня 2022г.
7	Министерство регионального развития Республики Алтай	выездная проверка	27 июня 2022г. - 1 июля 2022г.
8	Министерство природных ресурсов, экологии и туризма Республики Алтай	выездная проверка	4 июля 2022г. - 8 июля 2022г.
9	Министерство сельского хозяйства Республики Алтай	выездная проверка	11 июля 2022г. - 15 июля 2022г.
10	Комитет по охране, использованию и воспроизводству объектов животного мира Республики Алтай	выездная проверка	18 июля 2022г.- 22 июля 2022г.
11	Комитет по делам ЗАГС и архивов Республики Алтай	выездная проверка	25 июля 2022г. - 29 июля 2022г.
12	Комитет по тарифам Республики Алтай	выездная проверка	1 августа 2022г.- 5 августа 2022г.
13	Комитет по национальной политике и связям с общественностью Республики Алтай	выездная проверка	8 августа 2022г. - 12 августа 2022г.
14	Комитет по обеспечению деятельности мировых судей Республики Алтай	выездная проверка	15 августа 2022г.- 19 августа 2022г.
15	Комитет по физической культуре и спорту Республики Алтай	выездная проверка	22 августа 2022г.- 26 августа 2022г.
16	Комитет ветеринарии с Госветинспекцией Республики Алтай	выездная проверка	29 августа 2022г.- 2 сентября 2022г.
17	Комитет по гражданской обороне, чрезвычайным ситуациям и пожарной безопасности Республики Алтай	выездная проверка	5 сентября 2022г.- 9 сентября 2022г.
18	Инспекция по государственной охране объектов культурного наследия Республики Алтай	выездная проверка	12 сентября 2022г.- 16 сентября 2022г.

Приложение № 1
к приказу Министерства цифрового
развития Республики Алтай
от «29» декабря 2021 г. № 1294

Методические рекомендации оценки состояния системы защиты государственных информационных систем Республики Алтай и информационно-телекоммуникационной инфраструктуры исполнительных органов государственной власти Республики Алтай на 2022 год

I. Термины и определения

система защиты информации – совокупность у организаций и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

социальный инжиниринг – совокупность приёмов, методов и технологий создания такого пространства, условий и обстоятельств, максимально эффективно приводящей к конкретному необходимому результату с использованием социологии и психологии;

тестирование на проникновение – оценка безопасности информационной системы или компьютерных сетей средствами моделирования (имитации) действий потенциального злоумышленника (нарушителя);

уязвимость – недостаток в системе, используя который, можно намеренно нарушить ее целостность и вызвать неправильную работу;

уровень зрелости – этап развития организации в соответствии со стандартизованными моделями оценки уровня зрелости управления. Уровни проходятся последовательно и определяются различными характеристиками, включающими миссию, ценности, стратегию, организационную структуру;

хост – любое устройство, предоставляющее сервисы формата «клиент–сервер» в режиме сервера по каким–либо интерфейсам и уникально определённое на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключённый к локальной или глобальной сети;

СКЗИ – средства криптографической защиты информации;

иные понятия и термины, используемые в настоящих Методических рекомендациях, применяются в значениях, определенных федеральным законодательством в области защиты информации.

II. Общие сведения

1. Настоящие Методические рекомендации разработаны во исполнение пункта 4 решения расширенного заседания Совета по информационной безопасности при Главе Республики Алтай, Председателе Правительства Республики Алтай от 29 октября 2021 года (далее – Решение Совета по информационной безопасности) и определяют виды контроля состояния системы защиты информации и порядок проведения контроля состояния системы защиты информации.

2. Настоящие Методические рекомендации предназначены для организации работ по защите любой информации, за исключением сведений, составляющих государственную тайну.

3. Настоящие Методические рекомендации предназначены для исполнительных органов государственной власти Республики Алтай, включая подведомственные им учреждения (далее – ИОГВ РА) и не исключают обязанность исполнения требований по защите информации установленных федеральным законодательством.

III. Виды контроля состояния системы защиты информации

4. Контроль состояния системы защиты информации подразделяется на внешний и внутренний.

5. Внутренний контроль состояния системы защиты информации организуется и проводится сотрудниками, ответственными за обеспечение безопасности информации, определенными правовым актом ИОГВ РА (далее – ответственный за обеспечение безопасности информации).

6. Внешний контроль состояния систем защиты информации ИОГВ РА проводится Министерством цифрового развития Республики Алтай на основании Решения Совета по информационной безопасности в соответствии с планом проведения контроля состояния систем защиты государственных информационных системах Республики Алтай и информационно-телекоммуникационной инфраструктуры исполнительных органов государственной власти Республики Алтай на 2022 год, утверждаемым приказом Министерства цифрового развития Республики Алтай.

7. В целях подготовки к внешнему контролю состояния системы защиты рекомендуется определить ответственного за обеспечение безопасности информации в ИОГВ РА. Руководителям структурных подразделений ИОГВ РА оказывать всестороннее содействие в работе ответственного за обеспечение безопасности информации.

8. Мероприятия по контролю состояния защиты информации в ИОГВ РА включают проверку:

а) выполнение требований федерального законодательства в области защиты информации. Проводится оценка организационных мер (наличие и соответствие организационно распорядительных документов) и технических мер (наличие и состояние технических средств защиты информации). Проводится для процессов, в рамках которых обрабатывается информация ограниченного доступа, а также другая информация, если это установлено

федеральным законодательством (обработка персональных данных без использования средств автоматизации, служебное делопроизводство документов с пометкой «для служебного пользования», организация работ с средствами криптографической защитой информации, функционирование государственных информационных систем, информационных систем персональных данных и т.п.);

б) состояния защищенности локальной вычислительной сети ИОГВ РА. Оценка состояния защищенности локальной вычислительной сети может проводиться собственными силами и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Оценку состояния защищенности локальной вычислительной сети целесообразно проводить на любом уровне зрелости управления процессами информационной безопасности;

в) оценка уязвимостей информационно-телекоммуникационной инфраструктуры ИОГВ РА. Оценка уязвимостей проводится с целью выявления уязвимостей в системном и прикладном программном обеспечении для их дальнейшего устранения. Оценка уязвимостей может проводиться как собственными силами (оценку проводит ответственный за обеспечение безопасности информации), так с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Мероприятия по оценке уязвимостей могут проводиться ручными и инструментальными методами. Ручная оценка уязвимостей проводится путем проверки состояния созданных сервисов и версий программного обеспечения с дальнейшим изучением наличия в них уязвимостей путем сбора данных с общедоступных источников (банк данных угроз ФСТЭК России https://bdu.fstec.ru, база данных уязвимостей https://www.cvedetails.com, официальные сайты программного обеспечения и т.п.). Инструментальная оценка уязвимостей осуществляется с помощью специализированного программного обеспечения (сканеры сети, сканеры безопасности и т.п.);

г) проведение тестирования на проникновение. Тестирование на проникновение могут проводиться собственными силами и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

9. Типы тестирования на проникновение:

а) командное взаимодействие при проведении тестирования на проникновение. Мероприятия проводятся с одной стороны в режиме проведения реальных компьютерных атак (этичный хакинг) и противодействия атакам со стороны ответственных за обеспечение безопасности информации, с другой стороны. Целью проведения таких мероприятий является проверка эффективности деятельности ответственных за обеспечение безопасности информации, их квалификация, а также

выявления «узких» слабых мест в системе защиты информации. Командное взаимодействие целесообразно проводить на наивысшем уровне зрелости управления процессами информационной безопасности;

б) Тестирование на проникновение без участия ответственных за обеспечение безопасности информации.

10. Виды тестирования на проникновение:

а) внешнее тестирование на проникновение является имитацией компьютерных атак в отношении внешних информационных ресурсов подведомственного учреждения (информационные ресурсы, доступные со стороны информационно-телекоммуникационной сети «Интернет» – официальные сайты, внешние IP адреса, почтовые серверы и т.п.);

б) внутреннее тестирование на проникновение является имитацией действий злоумышленника после его проникновения в атакуемую локальную вычислительную сеть. Такой вид тестирования подразумевает повышение привилегий на захваченном хосте, разведка окружающих хостов с дальнейшими попытки их взлома;

в) тестирование на проникновение с применением методов социального инжиниринга проводится для проверки уровня осведомленности сотрудников подведомственного учреждениях в вопросах информационной безопасности. Это может быть имитация спам–рассылки через электронную почту, подкидывание флеш–накопителей с заранее записанными на них «вредоносными» программами, вытягивание данных учетных записей (имена пользователей и их пароли) путем маскировки под техническую поддержку и иные манипулятивные способы, направленные на психологические слабости, свойственные людям.

11. Целью проведения внешнего и внутреннего тестирования на проникновение является проверка защищенности информационных ресурсов на устойчивость к компьютерным атакам. Такие виды тестирования на проникновение возможно проводить на любом уровне зрелости управления процессами информационной безопасности с соблюдением следующего условия – целесообразно предварительно предупреждать сотрудников и (или) структурные подразделения, ответственные в подведомственном учреждении за информационные технологии.

12. Типовой перечень вопросов, рассматриваемых в ходе контроля выполнения требований федерального законодательства в области защиты информации приведен в приложении № 1 к настоящим Методическим рекомендациям. Приложенный типовой перечень не включает вопросы защиты объектов критической информационной инфраструктуры.

13. Типовой перечень вопросов, рассматриваемых в ходе оценки состояния защищенности локальной вычислительной сети приведен в приложении № 2 к настоящим Методическим рекомендациям.

14. Рекомендуемое содержание отчета по результатам тестирования на проникновение контроля согласно приложению № 3 к настоящим Методическим рекомендациям.

IV. Порядок проведения контроля состояния системы защиты информации

15. В ИОГВ РА разрабатывается документ, определяющий регламент проведения внутреннего контроля, предусматривающий особенности функционирования конкретного ИОГВ РА. В документе определяются ответственные исполнители (сотрудники, организующие и осуществляющие внутренний контроль), сроки проведения внутреннего контроля, виды и типы внутреннего контроля, перечень проверяемых вопросов, формы отчетности, порядок доведения результатов проведенных работ по руководителя ИОГВ РА, а также порядок устранения выявленных недостатков.

16. Общие рекомендации по проведению контроля.

17. Мероприятия по внешнему контролю состояния системы защиты информации включаются в ежегодный план организационно– технических мероприятий, утверждаемый Министерством цифрового развития Республики Алтай.

18. Тип и виды контроля, а также необходимость привлечения на договорной основе сторонних организаций, целесообразно выбирать исходя из квалификации ответственных за обеспечение безопасности информации, финансового обеспечения и текущих нужд ИОГВ РА.

19. Материалы проверки (справки, отчеты) содержат сведения о системе защиты информации, которым следует присваивать ограничительную пометку «для служебного пользования».

20. В случае выявления недостатков составляется план по их устранению.

21. Информацию о выявленных грубых нарушениях требований по защите информации, ставшая известной в ходе контрольных мероприятий, рекомендуется доводить до руководителя ИОГВ РА, а также включать в доклад на заседания Совета по информационной безопасности, для принятия управленческих решений.

Приложение №1
к Методическим рекомендациям оценки
состояния системы защиты
государственных информационных систем
Республики Алтай
и информационно-телекоммуникационной
инфраструктуры исполнительных органов
государственной власти
Республики Алтай на 2022 год

ТИПОВОЙ ПЕРЕЧЕНЬ

вопросов, рассматриваемых в ходе контроля выполнения требований федерального законодательства в области защиты информации

1. Организация защиты персональных данных.

а) выполнение требований Федерального закона от 27.07.2016 № 152–ФЗ «О персональных данных» (далее – ФЗ–152).

б) проверка сведений, содержащихся в уведомлении в соответствии с ч.3 ст. 22 ФЗ–152 (далее – уведомление).

2. Уведомление уполномоченного органа (Роскомнадзор) о начале обработки персональных данных и о внесении изменений в ранее представленные сведения осуществляется в соответствии с Приказом Роскомнадзора от 30.05.2017г. № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения».

Пункты ч. 3 ст. 22	Поле	Примечание
1	Наименование (фамилия, имя, отчество-при наличии), адрес оператора	Содержание соответствует установленным требованиям
2	Цель обработки персональных данных	Содержание соответствует установленным требованиям
3	Категории персональных данных	Содержание соответствует установленным требованиям
4	Категории субъектов, персональные данные которых обрабатываются	Содержание соответствует установленным требованиям
5	Правовое основание обработки персональных данных	Содержание соответствует установленным требованиям
6	Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных	Содержание соответствует установленным требованиям
7	Описание мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27.07.2006 № 152– ФЗ, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств	Содержание соответствует установленным требованиям
8	Фамилия, имя, отчество-при наличии физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их	Содержание соответствует установленным требованиям

Пункты ч. 3 ст. 22	Поле	Примечание
	контактных телефонов, почтовые адреса и адреса электронной почты	
9	Дата начала обработки персональных данных	Содержание соответствует установленным требованиям
10	Срок или условие прекращения обработки персональных данных	Содержание соответствует установленным требованиям
11	Сведения о наличии или об отсутствии трансграничной передачи персональных данных	Содержание соответствует установленным требованиям
12	Сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации	Содержание соответствует установленным требованиям
13	Сведения об обеспечении безопасности персональных данных	Содержание соответствует установленным требованиям

3. Выполнение организационных мер по ФЗ–152

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
1.	ч. 3 ст. 6 ФЗ–152	Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта	Наличие договоров (поручений) оператора с третьими лицами на обработку персональных данных
2.	ч. 4 ст. 9 ФЗ–152	Обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных	Наличие письменного согласия субъекта персональных данных на обработку персональных данных соответствующего требованиям законодательства Российской Федерации
3.	ст. 10 ФЗ–152	Выполнение условий обработки специальных категорий ПДн	Если ведется обработка, то необходимо: – наличие письменного согласия субъекта персональных данных на обработку специальных категорий персональных данных; – документальное подтверждение причин обработки в соответствии со статьей 10
4.	ст. 11 ФЗ–152	Выполнение условий обработки биометрических персональных данных	Если ведется обработка, то необходимо: – наличие письменного согласия субъекта персональных данных на обработку специальных категорий персональных данных; Российской Федерации документальное подтверждение причин обработки в соответствии со статьей 11
5.	ст. 12 ФЗ–152	Выполнение условий защиты при трансграничной передаче персональных данных	Если ведется передача, то необходимо: – наличие письменного согласия субъекта персональных данных на обработку специальных категорий персональных данных; – документальное подтверждение, что иностранным государством, на территорию которого осуществляется передача

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
			персональных данных, обеспечивается адекватная защита прав субъектов персональных данных
6.	ст. 18 ФЗ– 152	Обязанности оператора при сборе персональных данных	Наличие "Разъяснения субъекту персональных данных юридических последствий отказа предоставить его персональные данные". Выполнение записи, систематизации, накопления, хранения, уточнения (обновление, изменение), извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации
7.	ст. 18. 1 ФЗ– 152	Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом	Оператор обязан: 1) назначить ответственного за организацию обработки персональных данных; 2) издать документы: – определяющие политику оператора в отношении обработки ПДн (опубликовать или иным образом обеспечить неограниченный доступ к документу, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно– телекоммуникационной сети), Рекомендуемый параметр: документы, определяющие политику в отношении обработки персональных данных, соответствуют "Рекомендациям по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152– ФЗ "О персональных данных" (https://rkn.gov.ru/personal– data/p908/) – локальные акты по вопросам обработки ПДн, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений; 3) осуществлять внутренний контроль и (или) аудит соответствия обработки ПДн законодательству и локальным актам оператора; 4) провести оценку вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер; 5) проводить ознакомление работников оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства о ПДн и локальными актами по вопросам обработки ПДн.
8.	ст. 19 ФЗ– 152	Меры по обеспечению безопасности персональных данных при их обработке	1) разработка модели угроз безопасности ПДн при их обработке в информационных системах персональных данных;

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
			2) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации; 3) проведение оценки эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы персональных данных; 4) ведение учета машинных носителей персональных данных; 5) обнаружение фактов НСД к ПДн и принятие мер; 6) восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (регламент резервного копирования); 7) проведение периодического контроля за принимаемыми мерами по обеспечению безопасности ПДн и проведение оценки уровня защищенности информационных систем ПДн.
9.	п. 4 ст. 21 ФЗ– 152	Соответствие сроков хранения персональных данных целям их обработки	Проверка соответствия сроков хранения персональных данных целям их обработки (трудовой договор, договор на оказание услуг, журнал регистрации), порядок уничтожения.
10.	п. 3 ч. 4 ст. 22.1 ФЗ– 152	Лицо, ответственное за организацию обработки персональных данных, в частности, обязано организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов	Проверка организации приема и обработки обращений и запросов субъектов персональных данных или их представителей.

4. Выполнение требований Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687 (далее – требования Положения).

№ п/п	Пункт в требовании Положения	Требование нормативного документа	Рекомендации по возможной реализации требования
1.	Пункт 13	Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ	Приказ об определении мест хранения ПДн; Перечень лиц, осуществляющих обработку персональных данных. Документы по организации хранения, наличие и состояние сейфов, порядок закрытия и опечатывания сейфов. (Проверка соблюдения требований законодательства при обработке персональных данных работника кадровой службой. Ст. 85 – ст. 90 Трудового кодекса Российской Федерации. Указ президента Российской Федерации от 30.05.2005 № 609 "Об утверждении Положения о

№ п/п	Пункт в требовании Положения	Требование нормативного документа	Рекомендации по возможной реализации требования
			персональных данных государственного гражданского служащего РФ и ведении его личного дела)"
2.	Пункт 14	Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях	Организация раздельного хранения
3.	Пункт 15	При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором	Перечень лиц, имеющих доступ к местам хранения ПДн (Проверка наличия охраны помещений, в которых ведется работа с персональными данными (документы по оборудованию помещений средствами защиты))

5. Выполнение требований к защите персональных данных при их обработке в информационных системах персональных данных утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (далее – Требования к защите ПДн).

№ п/п	Пункт в Требованиях к защите ПДн	Требование нормативного документа	Рекомендации по возможной реализации требования
1.	Пункты 7,8	Определение типа угроз безопасности персональных данных, актуальных для информационной системы и уровня защищенности персональных данных	Акт определения уровня защищенности
2.	Пункты 13, 14, 15, 16	Выполнение требований пунктов по уровням	Проведение организационных и технических мероприятий по реализации требований по определенному уровню защищенности
3.	Пункт 17	Контроль за выполнением требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).	Организация контроля

6. Выполнение требований Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) от 18.02.2013 № 21 (далее – приказ ФСТЭК № 21).

№ п/п	Пункт в Приказе ФСТЭК № 21	Требование нормативного документа	Рекомендации по возможной реализации требования
1.	Пункт 4 приказа	Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия.	Наличие документов на средства защиты, подтверждающих проведение оценки соответствия
2.	Пункт 6 приказа	Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года	Наличие документов по оценке эффективности реализованных в рамках системы защиты ПДн, мер по обеспечению безопасности ПДн. Соблюдение периодичности оценки
3.	Пункт 8.1 приказа	Реализация меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21
4.	Пункт 8.2 приказа	Реализация меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21
5.	Пункт 8.3 приказа	Реализация меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21
6.	Пункт 8.4 приказа	Реализация меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным,	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с моделью угроз утвержденной в организации

№ п/п	Пункт в Приказе ФСТЭК № 21	Требование нормативного документа	Рекомендации по возможной реализации требования
		а также несанкционированное использование съемных машинных носителей персональных данных.	
7.	Пункт 8.5 приказа	Реализация меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с моделью угроз утвержденной в организации
8.	Пункт 8.6 приказа	Реализация меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с моделью угроз утвержденной в организации
9.	Пункт 8.7 приказа	Реализация меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с моделью угроз утвержденной в организации
10.	Пункт 8.8 приказа	Реализация меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с моделью угроз утвержденной в организации
11.	Пункт 8.9 приказа	Реализация меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с моделью угроз утвержденной в организации
12.	Пункт 8.10 приказа	Реализация меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу,	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с

№ п/п	Пункт в Приказе ФСТЭК № 21	Требование нормативного документа	Рекомендации по возможной реализации требования
		к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы	моделью угроз утвержденной в организации
13.	Пункт 8.11 приказа	Реализация меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с моделью угроз утвержденной в организации
14.	Пункт 8.12 приказа	Реализация меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с моделью угроз утвержденной в организации
15.	Пункт 8.13 приказа	Реализация меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно– телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с моделью угроз утвержденной в организации
16.	Пункт 8.14 приказа	Реализация меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с

№ п/п	Пункт в Приказе ФСТЭК № 21	Требование нормативного документа	Рекомендации по возможной реализации требования
		принятие мер по устранению и предупреждению инцидентов	моделью угроз утвержденной в организации
17.	Пункт 8.15 приказа	Реализация меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений	Реализация данной меры в соответствии с установленным уровнем защищенности (приложение) приказа ФСТЭК № 21 и в соответствии с моделью угроз утвержденной в организации
18.	Пункт 11 приказа	Реализация дополнительных мер защиты при наличии угроз 1– го и 2– го типов по Постановлению Правительства № 1119	Реализация данных мер согласно установленным требованиям
19.	Пункт 12 приказа	Соответствия классов защиты используемых средств защиты и СВТ, уровням защищенности ИСПДн	Проверка соответствия
20.	Пункт 13 приказа	При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 10 Приказа ФСТЭК № 21	Проверка соответствия (при наличии)

7. Выполнение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденного приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 рассмотрено в пункте 5.2 раздела «Организация защиты информации с использованием средств криптографической защиты информации».

8. Организация защиты информации, доступ к которой ограничен федеральными законами (за исключением сведений, составляющих государственную тайну).

9. Проверка выполнения требований «Специальных требований и рекомендаций по технической защите конфиденциальной информации», утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282 (далее – СТР–К) и Руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации», утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 (далее – РД АС Защита от НСД).

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
1.	п. 2.15 СТР– К	Наличие лиц, ответственных за обеспечение безопасности конфиденциальной информации, наличие в должностной инструкции обязанностей по защите информации.	Приказ о назначении
2.	п.п.3.6, 3.10, 5.1.3, 5.2.2 СТР–К; указ Президента Российской Федерации об утверждении перечня сведений конфиденциального характера от 6.03.1997 № 188	Наличие и содержание перечня сведений конфиденциального характера с учетом ведомственной и отраслевой специфики этих сведений, утвержденного руководителем организации. Ознакомление с перечнем сотрудников учреждения, организации, подведомственного органу исполнительной власти края (далее – ПУ) под роспись в части их касающейся	Наличие и соответствие перечня текущим условиям деятельности ПУ
3.	п. 2.4. СТР–К, п. 1.5. АС. Защита от НСД	Учет информационных ресурсов, подлежащих защите в АС, с указанием уровня конфиденциальности (объекты доступа)	Разработка документов: – перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности; – перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий; – матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС; – режим обработки данных в АС
4.	п.п. 2.16, 4.2.3, 5.1.3. СТР–К	Применение сертифицированных средств защиты информации либо сертифицированных технических средств обработки информации. Проверка актуальности и легитимности сертификатов соответствия на применяемые средства защиты информации	Наличие действующих сертификатов соответствия требованиям безопасности информацию
5.	п.3.4 СТР–К	Проверка договоров на проведение мероприятий по защите информации с организациями– лицензиатами, в случае проведения ими мероприятий по защите КИ (аттестация, контроль). Проверка наличия действующих лицензий организаций– лицензиатов	Наличие договоров

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
6.	п. 3.8 СТР–К	Приказ об определении объекта информатизации, в котором устанавливается необходимость обработки (обсуждения) конфиденциальной информации	Наличие
7.	п.п. 3.8, 2.13 СТР–К	Разработка модели угроз безопасности информации и модели вероятного нарушителя (ГОСТ Р 51275– 2006)	Наличие
8.	п.п.3.18, 3.8, 4.2.1, СТР–К	Наличие и правильность оформления Технического паспорта на объект информатизации. Наличия отметок о проведении контрольных мероприятий	Наличие
9.	п.п. 3.8, 3.15, 5.1.4, 5.1.7, 5.2.3, 5.4.2, 5.4.3 СТР–К. п.1.1. РД АС. Защита от НСД	Оценка правильности определения класса защищенности автоматизированных систем	– Приказ о назначении комиссии по классификации АС – Акт классификации, проверка классификационных признаков в соответствии с (перечнем защищаемых информационных ресурсов АС и их уровня конфиденциальности, перечня лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий, матрицы доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС, режима обработки данных в АС). Классификация ИСПДн не ниже классов 1Д, 2Б и 3Б соответственно
10.	п.п.3.16, 5.1.3 СТР–К	Порядок организации физической охраны	Наличие подразделения по физической охране (наименование организации, оказывающей услуги физической охраны, номер и дата договора). Наличие и содержание документов об организации пропускного и внутриобъектового режима
11.	п.п. 3.16, 4.2.1, 5.1.3, 5.2.7, 5.3.2, 5.6.6 СТР–К	Проверка наличия документов разрешительной системы доступа: – список лиц, допущенных к самостоятельной работе в АС (субъект доступа); – список лиц эксплуатационного (обслуживающего персонала) в ЗП, АС; – список лиц, имеющих право самостоятельного доступа в помещения, в которых обрабатывается (обсуждается) конфиденциальная информация; – наличие заявок на доступ к информационным ресурсам (должно быть прописано в документации по разрешительной системе допуска);	Наличие документов

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
		– перечень программного обеспечения, разрешенного к использованию в АС (субъект доступа)	
12.	п. 3.16 СТР–К	Наличие Приказа о назначении ответственных за эксплуатацию средств защиты информации (объекта информатизации).	Наличие документа
13.	п.п. 3.18, 5.5.1, 5.5.3, 5.5.5 СТР–К	Описание технологического процесса обработки информации. Наличие, содержание и сравнение с реальным технологическим процессом путем опроса исполнителей При использовании обработки информации с использованием МНИ должно быть обеспечено исключение хранения информации на ПЭВМ в нерабочее время.	Наличие документа, соответствие установленным требованиям
14.	п. 3.18 СТР–К	План организационно– технических мероприятий по подготовке объекта информатизации к внедрению средств и мер защиты информации.	Наличие плана
15.	п. 3.18, 5.3.1 "СТР–К"	Наличие и содержание документов: – инструкции пользователям АС по эксплуатации средств защиты информации – инструкции администратору АС по эксплуатации средств защиты информации – инструкции администратору безопасности АС по эксплуатации средств защиты информации.	Наличие документов
16.	п. 1.5 РД АС. Защита от НСД п.5.3.2, 5.1.3 СТР–К	Матрица доступа – наличие и проверка описанных в матрице и реальных прав в АС Реализация разграничения доступа к информационным ресурсам в соответствии с матрицей доступа.	Наличие документа и соответствие реального технологического процесса.
17.	п.2.17, СТР–К	Наличие аттестатов соответствия на объекты информатизации, обрабатывающие конфиденциальную информацию.	Наличие
18.	п.3.22 СТР–К	Наличие и содержание программы и методики проведения аттестационных испытаний.	Наличие
19.	п.3.20 СТР–К	Правильность проведения аттестационных испытаний наличие и содержание аттестационной документации.	Наличие
20.	п.3.21 СТР–К	Наличие правовых актов: – на проектирование объекта информатизации и назначение ответственных исполнителей; – на проведение работ по защите информации; – о назначении лиц, ответственных за эксплуатацию объекта информатизации;	Наличие

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
		– на обработку в АС (обсуждение в ЗП) конфиденциальной информации (правовой акт о вводе ОИ в эксплуатацию).	
21.	п.3.24 СТР–К	Организация контроля эффективности организационных и технических мероприятий по технической защите информации.	Наличие не реже 1 раза в год
22.	п.4.2.1 СТР–К	Наличие перечня защищаемых помещений.	Наличие
23.	п. 4.2.4 СТР–К	Проведение специальных проверок технических средств, установленных в защищаемых помещениях проводится при необходимости, по решению руководителя.	Наличие (рекомендовано)
24.	раздел 4.2 СТР–К	Принятые меры по технической защите защищаемых помещений (описание принятых мер).	Наличие
25.	п. 4.4.3 СТР–К	Приказ о назначении ответственного за хранение и использование аппаратуры звуко– и видеозаписи информации, и обеспечено хранение и использование этой аппаратуры, исключающее несанкционированный доступ к ней (при использовании звуко- и видеозаписи в ЗП).	Наличие
26.	п.п. 5.1.3, 5.2.7, 5.3.2 СТР–К	Документы, регламентирующие порядок допуска к конфиденциальной информации (например, Положение о разрешительной системе допуска).	Наличие
27.	п. 5.1.3 СТР–К	Порядок аудита событий в АС – проверка настроек СЗИ в части аудита в соответствии с установленным классом защищенности АС – указание в инструкциях администраторам АС о проведении аудита событий	Наличие
28.	п. 5.1.3 СТР–К	Опечатывание средств вычислительной техники, используемой в АС	Наличие
29.	п. 5.1.3 СТР–К	Организация резервного копирования: – правовой акт о назначении ответственного за резервное копирование; – инструкция по резервному копированию (с указанием периодичности резервирования, средств для осуществления резервного копирования, установленных носителей резервных копий)	Наличие
30.	п. 26 Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по	Приказ об определении контролируемой зоны в ПУ	Наличие

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
	техническим каналам от 15.09.1993 № 912– 51 (далее – Положение о ГСЗИ)		
31.	п. 5.1.3 СТР–К	Защита линий электропитания и заземления средствами активной защиты информации (в случае размещения трансформаторной подстанции за пределами контролируемой зоны)	Наличие
32.	п. 5.1.3 СТР–К	Использование сертифицированных систем гарантированного электропитания	Наличие
33.	п. п. 5.1.3, 5.2.5 СТР–К	Организация защиты конфиденциальной информации при ее передаче по каналам связи – использование средств криптографической защиты информации в случае передачи данных по незащищенным каналам связи; – размещение линий связи в пределах контролируемой зоны	Выполнение
34.	п.п. 5.1.3, 5.3.2 СТР–К	Размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр	Выполнение
35.	п. 5.1.3 СТР–К	Организация системы антивирусной защиты информации – назначение ответственных за антивирусную защиту информации – инструкция по антивирусной защите (с требованиями к антивирусным средствам, периодичностью антивирусного контроля) – проверка настроек средств антивирусной защиты.	Выполнение
36.	п.5.1.11 СТР–К	Проверка знаний сотрудников организаций по вопросам организации порядка обеспечения защиты конфиденциальной информации: – наличие нормативной законодательной базы по защите информации (Федеральные законы, методические документы, локальные нормативные правовые акты и так далее); – ознакомление с нормативными документами по защите информации в организации в части их касающейся (законодательные акты); – ознакомление сотрудников организации с внутренними документами по защите конфиденциальной информации (приказы, инструкции и т.п.) под роспись в части их касающейся.	Наличие документов, подтверждающих ознакомление и проверку
37.	п. 5.2.4 СТР–К	Наличие сертификатов на	Наличие

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
		используемые СВТ по электромагнитной совместимости, по безопасности, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216– 91, ГОСТ Р 50948– 96, ГОСТ Р 50949– 96, ГОСТ Р 50923– 96, СанПиН 2.2.2.542– 96)	
38.	п.5.3.2 СТР–К	Проверка организации стирания остаточной информации. Данное требование должно быть прописано в инструкциях пользователям/администраторам АС. Проверка работоспособности функции затирания информации в средствах защиты информации	Наличие
39.	п. 5.6.3 СТР–К	Проверка наличия средств защиты информации во всех узлах ЛВС независимо от наличия (отсутствия) в них конфиденциальной информации. В случае если АС не отделена от остальной ЛВС межсетевым экраном	Наличие
40.	п.п.5.3.2, 5.6.7 СТР–К	Организация парольной защиты	Наличие
41.	п.п. 5.7.2, 5.7.3 СТР–К	Использование в АС типа ЛВС средств обнаружения вторжений, мониторинга сети, активного аудита (в случае отсутствия подключения АС к сети Интернет). Разделение траффика на сетевом уровне с учетом решаемых задач пользователей. Проверка соответствия технологического процесса обработки информации правилам фильтрации межсетевых экранов	Наличие
42.	п.5.8.2. СТР–К	Проверка настроек штатных средств защиты в СУБД	Наличие
43.	п.5.6.5. СТР–К п.1 Указа Президента Российской Федерации от 17.03.2008 г. № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно – телекоммуникационных сетей международного информационного обмена" (далее – Указ № 351)	Использование сертифицированных межсетевых экранов соответствующего класса согласно установленного класса защищенности АС	Наличие
44.	п.п.6.1.4, 6.2.1, 6.3.2, 6.3.3, 6.3.4, 6.3.6, 6.3.8, 6.3.9, 6.3.11 СТР–К	Порядок использования в АС сети Интернет	Использование электронной подписи при передаче конфиденциальной информации для подтверждения подлинности, использование средств обнаружения вторжений, сокрытие топологии сети путем фильтрации на сетевом уровне,

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
			использование средств анализа защищенности АП, – использование средств усиленной идентификации и аутентификации, – централизованное управление системой защиты информации, наличие Приказа о допуске к работе на АП, Приказ о назначении администратора безопасности, ознакомление исполнителей с требованиями по защите информации при подключении АС к сети Интернет, наличие инструкции, регламентирующей порядок допуска к сети Интернет, содержание инструкции, наличие заявок на допуск к сети Интернет, содержание заявок, Приказ о назначении комиссии по приемке в эксплуатацию АП, заключение о выполнении требований по защите информации при подключении АС к сети Интернет, содержание заключения, Приказ об организации контроля защиты информации в АС, имеющей подключение к сети Интернет.
45.	п.п.6.3.13.1, 6.3.13.2, 6.3.13.3 СТР–К	Обеспечение безопасности информации при удаленном доступе к ресурсам АП.	Наличие
46.	п.п. 6.3.14.1, 6.3.14.2, 6.3.14.3, 6.3.15, 6.3.15.1, 6.3.15.2 СТР–К	Обеспечение безопасности информации при межсетевом взаимодействии отдельных АП одной организации через сеть Интернет	
47.	п.2.5 РД АС. Защита от НСД	Выполнение требований по защите конфиденциальной информации, обрабатываемой в АС класса защищенности 3Б; – подсистема управления доступом; – подсистема регистрации и учета; – подсистема обеспечения целостности	Выполнение
48.	п.2.8 РД АС. Защита от НСД	Выполнение требований по защите конфиденциальной информации, обрабатываемой в АС класса защищенности 2Б: – подсистема управления доступом; – подсистема регистрации и учета; – подсистема обеспечения целостности	Выполнение
49.	п.2.11 РД АС. Защита от НСД	Выполнение требований по защите конфиденциальной информации, обрабатываемой в АС класса защищенности 1Д: – подсистема управления доступом;	Выполнение

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
		– подсистема регистрации и учета; – подсистема обеспечения целостности	
50.	п.2.12 РД АС. Защита от НСД	Выполнение требований по защите конфиденциальной информации, обрабатываемой в АС класса защищенности 1Г: – подсистема управления доступом; – подсистема регистрации и учета; – подсистема обеспечения целостности	Выполнение

10. Сведения об обеспеченности и потребности в специалистах по информационной безопасности с требуемым уровнем подготовки.

№ п/п	Требование	Примечание
1.	Статус подразделения по ЗИ	В штатном расписании должно быть создано подразделение по ЗИ, либо должны быть назначены ответственные по защите конфиденциальной информации.
2.	Сведения о подготовке специалистов по ЗИ	Ответственные по ЗИ должны проходить курсы повышения квалификации не реже чем раз в три года.

11. Выполнение требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17 (далее – приказ ФСТЭК № 17).

№ п/п	Пункт в приказе ФСТЭК № 17	Требование нормативного документа	Рекомендации по возможной реализации требования
1.	п.9	Для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации	Выполнение требования в полном объеме
2.	п.11	Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации	Выполнение требования в полном объеме
3.	п.14	Формирование требований к защите информации, содержащейся в информационной системе	Формирование требований к защите информации, содержащейся в информационной системе включает: – принятие решения о необходимости защиты информации, содержащейся в информационной системе;

№ п/п	Пункт в приказе ФСТЭК № 17	Требование нормативного документа	Рекомендации по возможной реализации требования
			– классификацию информационной системы по требованиям защиты информации (далее – классификация информационной системы); – определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации; – определение требований к системе защиты информации информационной системы
4.	п.15	Разработка системы защиты информации информационной системы	Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы и включает: – проектирование системы защиты информации информационной системы; – разработку эксплуатационной документации на систему защиты информации информационной системы; – макетирование и тестирование системы защиты информации информационной системы (при необходимости)
5.	п.16	Внедрение системы защиты информации информационной системы	Осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает: – установку и настройку средств защиты информации в информационной системе; – разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (далее – организационно– распорядительные документы по защите информации); – внедрение организационных мер защиты информации; – предварительные испытания системы защиты информации информационной системы; – опытную эксплуатацию системы защиты информации информационной системы; – анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению; – приемочные испытания системы защиты информации информационной системы.
6.	п.17	Аттестация информационной системы по требованиям защиты информации (далее – аттестация информационной системы) и ввод ее в действие	В качестве исходных данных, необходимых для аттестации информационной системы, используются: – модель угроз безопасности информации;

№ п/п	Пункт в приказе ФСТЭК № 17	Требование нормативного документа	Рекомендации по возможной реализации требования
			– акт классификации информационной системы; – техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы; – проектная и эксплуатационная документация на систему защиты информации информационной системы; – организационно– распорядительные документы по защите информации; – результаты анализа уязвимостей информационной системы; – материалы предварительных и приемочных испытаний системы защиты информации информационной системы; – иные документы, разрабатываемые в соответствии с настоящими требованиями. Аттестация информационной системы проводится в соответствии с программой и методиками аттестационных испытаний. По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям о защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний.
7.	п.18	Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы	осуществляется оператором и включает: – управление (администрирование) системой защиты информации информационной системы; – выявление инцидентов и реагирование на них; – управление конфигурацией аттестованной информационной системы и ее системы защиты информации; – контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе
8.	п.19	Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации	Осуществляется оператором и включает: – архивирование информации, содержащейся в информационной системе; – уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.
9.	п. 20.1	Реализация мер по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17

№ п/п	Пункт в приказе ФСТЭК № 17	Требование нормативного документа	Рекомендации по возможной реализации требования
		присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности)	
10.	п. 20.2	Реализация мер по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17
11.	п. 20.3	Реализация мер по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска, запрещенного к использованию в информационной системе программного обеспечения	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17
12.	п. 20.4	Реализация мер по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17
13.	п. 20.5	Реализация мер по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17
14.	п. 20.6	Реализация мер по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17

№ п/п	Пункт в приказе ФСТЭК № 17	Требование нормативного документа	Рекомендации по возможной реализации требования
		информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации	
15.	п. 20.7	Реализация мер по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17
16.	п. 20.8	Реализация мер по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17
17.	п. 20.9	Реализация мер по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17
18.	п. 20.10	Реализация мер по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17

№ п/п	Пункт в приказе ФСТЭК № 17	Требование нормативного документа	Рекомендации по возможной реализации требования
19.	п. 20.11	Реализация мер по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17
20.	п. 20.12	Реализация мер по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17
21.	п. 20.13	Реализация мер по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно–телекоммуникационными сетями посредством применения	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17

№ п/п	Пункт в приказе ФСТЭК № 17	Требование нормативного документа	Рекомендации по возможной реализации требования
		архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации	
22.	п. 26	Технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих необходимые функции безопасности	Реализация данной меры в соответствии с установленным классом защищенности (приложение) приказа ФСТЭК № 17
23.	п. 27	В случае обработки в информационной системе информации, содержащей персональные данные, реализуемые в соответствии с пунктами 21 и 22 настоящих Требований меры защиты информации: – для информационной системы 1 класса защищенности обеспечивают 1, 2, 3 и 4 уровни защищенности персональных данных (устанавливается в соответствии с Требованиями к защите ПДн); – для информационной системы 2 класса защищенности обеспечивают 2, 3 и 4 уровни защищенности персональных данных; – для информационной системы 3 класса защищенности обеспечивают 3 и 4 уровни защищенности персональных данных	Реализация уровней защищенности в соответствии с классами защищенности

12. Организация защиты информации с использованием средств криптографической защиты информации. Выполнение инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну утвержденной приказом Федерального агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 (далее – Инструкция ФАПСИ).

№ п/п	Пункт в Инструкции ФАПСИ	Требование нормативного документа	Рекомендации по возможной реализации требования
1.	п. 21	Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к	Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией.

№ п/п	Пункт в Инструкции ФАПСИ	Требование нормативного документа	Рекомендации по возможной реализации требования
		самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего органа криптографической защиты на основании принятых от этих лиц зачетов по программе обучения.	В случае если ПУ является органом криптографической защиты информации
2.	п. 26	Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленным формам. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно–программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.	Наличие журнала учета
3.	п. 27	Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность	Журнал учета должен быть заполнен
4.	п. 30	Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей	Запираемые (а желательно и опечатываемые) ящики, шкафы, сейфы
5.	п. 51	Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее – спецпомещения), должны обеспечивать сохранность конфиденциальной информации, СКЗИ, ключевых документов	Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных

№ п/п	Пункт в Инструкции ФАПСИ	Требование нормативного документа	Рекомендации по возможной реализации требования
			на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения. В случае если ПУ является органом криптографической защиты информации
6.	п. 62	Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ	Реализация требования режимными мерами. В случае если ПУ является органом криптографической защиты информации
7.	п. 63	Режим охраны спецпомещений пользователей СКЗИ, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает обладатель конфиденциальной информации по согласованию с соответствующим органом криптографической защиты	Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции, специфику и условия работы конкретных пользователей СКЗИ. В случае если ПУ является органом криптографической защиты информации
8.	п. 64, п. 66	В спецпомещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ	У каждого пользователя должен быть свой (индивидуальный) опечатываемый шкаф. В обычных условиях опечатанные хранилища пользователей СКЗИ могут быть вскрыты только самими пользователями. В случае если ПУ является органом криптографической защиты информации
Требования, предъявляемые к организациям, в которых вырабатываются ключи шифрования (подписи). В случае если ПУ является органом криптографической защиты информации			
9.	пп. 52– 59	Проверка выполнения требований к помещениям, в которых генерируются ключи шифрования (подписи)	Режим, двери, окна, порядок сдачи под охрану, наличие металлических хранилищ
10.	п. 6	Назначение лица ответственного за криптографическую защиту информации	Приказ

№ п/п	Пункт в Инструкции ФАПСИ	Требование нормативного документа	Рекомендации по возможной реализации требования
		(орган криптографической защиты информации)	
11.	п. 13	Проверка соответствия подготовки специалиста, назначенного ответственным за криптографическую защиту информации требованиям по уровню подготовки.	Наличие сведений об обучении

13. Выполнение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10.07.2014 г. № 378 (далее – приказ ФСБ № 378).

Приказ ФСБ № 378 предназначен для операторов, использующих СКЗИ для обеспечения безопасности персональных данных при их обработке в информационных системах и определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах ПДн с использованием СКЗИ, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности.

Применение организационных и технических мер, определенных в настоящем документе, обеспечивает оператор с учетом требований эксплуатационных документов на СКЗИ, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах.

№ п/п	Пункты в приказе ФСБ № 378	Требование нормативного документа	Рекомендации по возможной реализации требования
Для обеспечения 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований			
1.	п. 5	Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	Необходимо обеспечение режима, которое достигается путем: а) оснащения Помещений входными дверьми с замками, обеспечения постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений;

№ п/п	Пункты в приказе ФСБ № 378	Требование нормативного документа	Рекомендации по возможной реализации требования
			б) утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях; в) утверждения перечня лиц, имеющих право доступа в Помещения.
2.	п. 5	Обеспечение сохранности носителей персональных данных	Осуществление хранения съемных машинных носителей ПДн в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. Осуществление поэкземплярного учета машинных носителей ПДн, который достигается путем ведения журнала учета носителей ПДн с использованием регистрационных (заводских) номеров
3.	п. 5	Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	Необходимо разработать и утвердить документ, определяющий перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей; Поддерживать в актуальном состоянии документ, определяющий перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей
4.	п. 5	Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	Использование для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше
Для обеспечения 3 уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований для предыдущего уровня защищенности необходимо выполнение следующих требований			
5.	п. 16	Назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе	Назначение обладающего достаточными навыками должностного лица (работника) оператора ответственным за обеспечение безопасности персональных данных в информационной системе
6.	п. 18	Использование СКЗИ класса КВ и выше в случаях, когда для информационной системы актуальны угрозы 2 типа. Использование СКЗИ класса КС1 и выше в случаях, когда для информационной системы актуальны угрозы 3 типа	Данная мера выполняется вместо данной в п. 4 таблицы

№ п/п	Пункты в приказе ФСБ № 378	Требование нормативного документа	Рекомендации по возможной реализации требования
Для обеспечения 2 уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований для предыдущего уровня защищенности необходимо выполнение следующих требований			
7.	п. 19	Необходимо выполнение требования о том, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей	а) утверждение руководителем оператора списка лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии; б) обеспечение информационной системы автоматизированными средствами, регистрирующими запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам в электронном журнале сообщений; в) обеспечение информационной системы автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений; г) обеспечение периодического контроля работоспособности указанных в подпунктах "б" и "в" настоящего пункта автоматизированных средств (не реже 1 раза в полгода)
8.	п. 21	Использование СКЗИ класса КА в случаях, когда для информационной системы актуальны угрозы 1 типа; Использование СКЗИ класса КВ и выше в случаях, когда для информационной системы актуальны угрозы 2 типа; Использование СКЗИ класса КС1 и выше в случаях, когда для информационной системы актуальны угрозы 3 типа	Данная мера выполняется вместо указанной в п. 4 настоящей таблицы
Для обеспечения 1 уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований для предыдущего уровня защищенности необходимо выполнение следующих требований			
9.	п. 22	Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе	а) обеспечение информационной системы автоматизированными средствами, позволяющими автоматически регистрировать в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе; б) отражение в электронном журнале безопасности полномочий сотрудников оператора персональных данных по доступу к персональным данным, содержащимся в информационной системе. Указанные полномочия должны

№ п/п	Пункты в приказе ФСБ № 378	Требование нормативного документа	Рекомендации по возможной реализации требования
			соответствовать должностным обязанностям сотрудников оператора; в) назначение оператором лица, ответственного за периодический контроль ведения электронного журнала безопасности и соответствия, отраженных в нем полномочий сотрудников оператора их должностным обязанностям (не реже 1 раза в месяц)
10.	п. 22	Создание отдельного структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение его функций на одно из существующих структурных подразделений	а) проведение анализа целесообразности создания отдельного структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе; б) создание отдельного структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение его функции на одно из существующих структурных подразделений
11.	п. 25	Дополнительные требования по организации режима обеспечения безопасности помещений, в которых размещена информационная система	а) оборудование окон Помещений, расположенные на первых и (или) последних этажах зданий, а также окон Помещений, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения; б) оборудование окон и дверей Помещений, в которых размещены серверы информационной системы, металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения.
12.	п. 25	Использование СКЗИ класса КА в случаях, когда для информационной системы актуальны угрозы 1 типа; Использование СКЗИ класса КВ и выше в случаях, когда для информационной системы актуальны угрозы 2 типа.	Данная мера выполняется вместо указанной в п. 4 таблицы

14. Организация защиты информации, размещаемой в информационно-телекоммуникационной сети «Интернет». Выполнение требований Федерального закона Российской Федерации «Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149–ФЗ (далее ФЗ – 149).

№ п/п	Наименование нормативного документа	Требование нормативного документа	Рекомендации по возможной реализации требования
1.	подпункт 1, п. 1 статьи 16 ФЗ – 149	Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; Реализация права на доступ к информации	Проверка на наличие "дублирующих" сайтов ПУ ("дублирующий" сайт – сайт, ложно или без ведома ПУ, публикующий информацию о его деятельности, замаскированный под официальный сайт ПУ или сайт, им созданный). Рекомендуемый параметр – отсутствуют. При невозможности закрытия таких сайтов необходимо обращаться в уполномоченные органы государственной власти
2.	подпункт 2 пункта 4 статьи 6 ФЗ – 149	Обладатель информации при осуществлении своих прав обязан принимать меры по защите информации	"Размещение информации ограниченного доступа на веб–сайте в непредназначенных для ее размещения разделах Необходимый параметр – информация ограниченного доступа в непредназначенных для ее размещения разделах отсутствует"

Приложение №2
к методическим рекомендациям оценки
состояния системы защиты
государственных информационных систем
Республики Алтай
и информационно-телекоммуникационной
инфраструктуры исполнительных органов
государственной власти
Республики Алтай на 2022 год

ТИПОВОЙ ПЕРЕЧЕНЬ
вопросов, рассматриваемых в ходе оценки состояния защищенности локальной вычислительной сети

Для проведения контрольных мероприятий в области защиты внутренних сетевых информационных ресурсов целесообразно рассматривать следующие исходные данные:

– логическая схема локальной вычислительной сети ИОГВ РА (далее – ПУ);

– физическая схема локальной вычислительной сети ПУ (далее – ЛВС);

– описание всех серверов (имя, операционная система, IP адрес, назначение);

– перечень IP– адресов и DNS– имен всех внешних информационных ресурсов, доступных со стороны информационно-телекоммуникационной сети «Интернет» по веб–интерфейсу (веб– сайты);

– перечень IP– адресов внутренней сетевой адресации ЛВС;

– полный перечень информационных систем, используемых в ПУ, в том числе, созданных самостоятельно (архитектура, количество серверов, тип (физический, виртуальный), операционная система), описание технологического процесса обработки информации (наличие выхода в сеть Интернет, количество точек подключения, описание контрагентов (организаций, работающих с информационной системой), способ подключения к информационной системе), сведения об используемых хэш–функциях для хеширования паролей (в виде фрагмента исходного кода) (для информационных систем собственной разработки);

В ходе контрольных мероприятий проводится анализ следующих блоков:

1. Политики безопасности паролей и блокировки учетных записей (доменные и локальные политики, Linux– серверы).

Проверяются серверы и критические приложения (например, контроллер домена, сервер управления базами данных, веб– сервер и т.п.).

№ п/п	Вопрос проверки	Результат проверки
1.	Максимальный срок действия пароля	Рекомендуемый параметр – не более 90 дней
2.	Минимальный срок действия пароля	Рекомендуемый параметр – не менее 60 дней

№ п/п	Вопрос проверки	Результат проверки
3.	Установка требований к сложности пароля	Рекомендуемый параметр – включена, наличие верхнего, нижнего регистра, наличие цифровых значений
4.	Минимальная длина пароля	Рекомендуемый параметр – не менее 8 символов
5.	Ведение журнала запоминания паролей	Рекомендуемый параметр – не менее 5 последних паролей
6.	Время до сброса счетчика блокировки	Рекомендуемый параметр – не менее 30 минут
7.	Пороговое значение блокировки	Рекомендуемый параметр – 6 ошибок входа в систему
8.	Продолжительность блокировки учетной записи	Рекомендуемый параметр – 30 минут
9.	Использование блокирование сеанса при установленном тайм– ауте бездействия	Рекомендуемый параметр – 15 минут
10.	Используемые хэш– функции (для ОС Windows)	Рекомендуемый параметр – используются NTLM– хеши, возможность использования LM– хешей отсутствует. В системном реестре ОС ключу NoLmHash ветки реестра HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Control\Lsa присвоено значение 1

* Проверке не подлежат устройства и системы, которые преднастроены производителем (например, системы хранения данных). Веб– приложения таких систем подлежат проверке по параметрам безопасности, встроенным в эти приложения.

2. Наличие настроек и паролей по умолчанию.

Проверка проводится путем сканирования сети сканером типа "nmap", изучением открытых портов и служб. Проверка использования паролей по умолчанию проводится путем подбора паролей по словарю.

№ п/п	Вопрос проверки	Результат проверки
1.	Наличие устройств в локальной сети с доступным интерфейсом управления, в котором отсутствует необходимость для рядовых сотрудников (например, веб– интерфейс периферийного оборудования)	Рекомендуемый параметр – доступ к интерфейсам управления отсутствует (для периферийного оборудования возможно изменение паролей административных учетных записей, встроенных по умолчанию)
2.	Наличие пароля, установленного по умолчанию на интерфейсах управления оборудования (например, беспарольный вход учетной записи SA в СУБД)	Рекомендуемый параметр – пароли изменены на всех интерфейсах (WEB, SSH, толстые клиенты СУБД и т.п.)

3. Использование небезопасных протоколов.

№ п/п	Вопрос проверки	Результат проверки
1.	Наличие FTP серверов (21 порт протокола TCP)	Возможные рекомендуемые параметры: – FTP отсутствует – для передачи файлов используются защищенные версии протокола FTP, например, SFTP – FTP используется, но обмен осуществляется только внутри сертифицированной ФСБ России VPN– сети
2.	Наличие открытых telnet портов (23 порт протокола TCP)	Рекомендуемый параметр – протокол telnet не используется. Для доступа к административной консоли применяется SSH.

№ п/п	Вопрос проверки	Результат проверки
3.	Использование протоколов обнаружения соседних устройств (Neighbor Discovery protocol) на пограничном сетевом оборудовании	Рекомендуемый параметр – выключено
4.	Доступ к веб– интерфейсам управления критическим ресурсами извне (например, наличие доступа к административной консоли пограничного маршрутизатора по веб– интерфейсу или протоколу SSH).	Рекомендуемый параметр – доступ по веб– интерфейсу или протоколу SSH отсутствует Возможно наличие доступа по защищенному каналу (VPN)

4. Использование беспроводных сетей.

№ п/п	Вопрос проверки	Результат проверки
1.	Использование беспроводных точек доступа	Возможные рекомендуемые параметры: – точки беспроводного доступа отсутствуют; – настройки точка доступа соответствуют рекомендуемым параметрам
2.	Использование WPS	Рекомендуемый параметр – отключено
3.	Используемые механизмы защиты доступа	Рекомендуемый параметр – WPA3[1], остальные протоколы считаются небезопасными
4.	Возможность доступа к внутренним ресурсам	Рекомендуемый параметр – отсутствует
5.	Избыточное применение беспроводных технологий (наличие включенных Wi– Fi интерфейсов на сетевом, периферийном и другом оборудовании, при наличии проводного соединения)	Рекомендуемый параметр – отсутствует

5. Безопасность ЛВС и информационных систем (при наличии информационных систем собственных разработок, собственных ЛВС).

Например, официальные сайты или иные веб– ресурсы, информационные системы для обмена данных с клиент– серверной архитектурой и т.п.

№ п/п	Вопрос проверки	Результат проверки
1	Для веб– ресурсов, к которым есть доступ со стороны сети Интернет	
2	Использование шифрования при передаче данных по открытым каналам связи	Рекомендуемый параметр – наличие действующего SSL– сертификата, полученного от доверенного (публичного) центра сертификации, шифрующего весь трафик (пользовательский и администраторский)
3	Длина открытого ключа SSL– сертификата	Рекомендуемый параметр – не менее 2048 бит, при технической возможности генерации ключа с большей длинной – 4096 бит
4	Длина ключа потокового шифрования	Рекомендуемый параметр – не менее 128 бит
5	спользование криптографических шифров и алгоритмов обмена ключами (не допускается применение алгоритмов блочного шифрования RC4 и DES)	Рекомендуемый параметр – класс А, полученный по результатам исследования веб– ресурса (например, через SSL Server Test (https://www.ssllabs.com/ssltest/ https://www.htbridge.com/ssl/)) и отсутствие

[1] Протокол WPA2 в 2018 году признан скомпрометированным

№ п/п	Вопрос проверки	Результат проверки
		несоответствия со стандартом PCI DSS (раздел "Test your servers for security and compliance with PCI DSS")
6	Использование криптостойких алгоритмов соединения ("рукопожатия")	Рекомендуемый параметр – использование варианта протокола Диффи–Хеллмана ECDHE
7	Версии криптоалгоритмов	Рекомендуемый параметр – TLS версий 1.1., 1.2., 1.3. Примечание – допускается применение TLS версий 1.0. на веб– ресурсах, используемых большим количеством жителей Российской Федерации ввиду невозможности работы более новых версий на старых устройствах. На веб– ресурсах, незадействованных для общественного использования, TLS версии 1.0. применять не рекомендуется.
8	Управление уязвимостями	Проверяются все веб– ресурсы ПУ вне зависимости от его принадлежности к статусу государственного информационного ресурса Рекомендуемый параметр – уязвимости отсутствуют.
9	Применяемые хэш–функции	Не допускается использовать хэш– функции SHA– 1, MD2, MD5. Рекомендуемый параметр – SHA– 2, SHA– 3, bcrypt/scrypt
10	Применение дополнительных мер защиты хеша пароля	Рекомендуемый параметр – генерация хеша пароля осуществляется с помощью криптостойкой хэш–функции с добавлением "соли". Местоположение "соли" при генерации окончательного хеша пароля – после пароля.
11	Использование загружаемого контента на веб– ресурсе (JavaScript сценариев, CSS файлов, файлов шрифтов и др.)	Рекомендуемый параметр – – контент хранится на сервере, обслуживающем сайт; – контент хранится на доверенных ресурсах (например, ссылки на ресурсы yandex.ru).
12	Реализация механизма сокрытия символов вводимого пароля	Рекомендуемый параметр –используется (например, символ *)
13	Использование счетчиков посещаемости	Рекомендуемый параметр – используемые счетчики, предоставляются юридическими лицами, зарегистрированными на территории Российской Федерации
14	Управление обновлениями программного обеспечения	Рекомендуемый параметр – все программное обеспечение обновлено до последней актуальной версии и поддерживается производителем
15	Защита от атак перебора пароля	Рекомендуемый параметр – доступ ограничивается после заданного количества неудачных попыток (не более 5 попыток)
16	Доступ к административным консолям, необходимость в котором в сети Интернет отсутствует (например, phpmyadmin или административный порт https://myhost.ru:8443, доступ к которому ограничен межсетевым экраном)	Рекомендуемый параметр – возможность доступа отсутствует
17	Защита от SQL– атак, XSS, CSRF	Рекомендуемый параметр – реализована (либо на 100% реализована фильтрация вводимых данных, либо установлен, настроен и включен в режим активной защиты межсетевой экран для веб– приложений)
18	Удаленное администрирование веб– ресурса	Рекомендуемый параметр – управление осуществляется через сертифицированную ФСБ России сеть VPN
19	Реализация механизма запрета одновременного запуска более одного сеанса из– под одной учетной записи	Рекомендуемый параметр – механизм реализован, используется

№ п/п	Вопрос проверки	Результат проверки
	Для информационных систем, разработанных сторонними разработчиками (за исключением "коробочных" решений)	
20	Защита каналов связи при подключении ИС в сети Интернет	Рекомендуемый параметр – подключение к ИС осуществляется по защищенному каналу связи без применения технологии "человек– по– середине" (например, OpenVPN)
21	Реализация механизма задания максимального срока действия пароля	Рекомендуемый параметр – механизм реализован, используется – не более 90 дней
22	Реализация механизма задания минимального срока действия пароля	Рекомендуемый параметр – механизм реализован, используется – не менее 60 дней
23	Реализация механизма задания минимального срока действия пароля	Рекомендуемый параметр – механизм реализован, используется – 18 дней
24	Реализация механизма задания минимальной длины пароля	Рекомендуемый параметр – механизм реализован, используется – не менее 8 символов
25	Реализация механизма задания сложности пароля	Рекомендуемый параметр – механизм реализован, используется – нижний/верхний регистр, цифровые значения, спецсимволы.
26	Реализация механизма ограничения ввода ранее введенного пароля при его смене	Рекомендуемый параметр – механизм реализован, используется – запоминается не меньше 5 последних паролей
27	Реализация механизма задания времени до сброса счетчика блокировки	Рекомендуемый параметр – механизм реализован, используется – не менее 30 минут
28	Реализация механизма задания порогового значения блокировки	Рекомендуемый параметр – механизм реализован, используется – не более 6 ошибок входа в систему
29	Реализация механизма задания продолжительности блокировки учетной записи	Рекомендуемый параметр – механизм реализован, используется – 30 минут
30	Реализация механизма сокрытия вводимого пароля	Рекомендуемый параметр – механизм реализован, используется – например символ *
31	Реализация механизма блокировки сеанса пользователя при заданном времени бездействия	Рекомендуемый параметр – механизм реализован, используется – не более 15 минут
32	Реализация механизма запрета одновременного запуска более одного сеанса из– под одной учетной записи	Рекомендуемый параметр – механизм реализован, используется
33	Для серверов информационных систем и ЛВС (контроллеры домена, сервера баз данных, файловые сервера, критической инфраструктуры)	
34	(Для операционных систем Windows) Использование встроенных учетных записей (администратор, гость)	Рекомендуемый параметр – отсутствуют
35	(Для операционных систем Linux) Возможность входа под учетной записью root через SSH	Рекомендуемый параметр – возможность отсутствует
36	Использование только персональных учетных записей каждым сотрудником	Рекомендуемый параметр – все сотрудники используют только свои персональные учетные записи
37	Использование доверенного DNS– сервера, в том числе для пользовательского трафика	Возможные рекомендуемые параметры – используется доверенный вышестоящий DNS Управления ФСБ России по Хабаровскому краю – используется доверенный DNS сервер юридического лица, являющегося резидентом Российской Федерации, оказывающего услугу облачного интернет– сервиса по контент– фильтрации – используется собственный DNS сервер, связанный с доверенным вышестоящим DNS сервером
38	Ограничение пользовательских привилегий	Рекомендуемый параметр – пользователи имеют привилегии, необходимые только для выполнения своих должностных обязанностей (обычные работники

№ п/п	Вопрос проверки	Результат проверки
		– привилегия "пользователь", администраторы – привилегия "локальный администратор", "администратор домена" и т.п.)
39	Для "коробочных" (готовых) решений (например, системы хранения данных, почтовые серверы в виде виртуальной машины с преднастроенной производителем (разработчиком) операционной системой и т.п.)	
40	Использование встроенных механизмов безопасности (требования к паролям, смена пароля по умолчанию, антивирусная защита (при наличии), блокировка попыток доступа и т.п.)	Рекомендуемый параметр – встроенные механизмы безопасности должны использоваться в полном объеме.

6. Работа систем межсетевого экранирования (сайты, критические ресурсы).

№ п/п	Вопрос проверки	Результат проверки
1.	Сетевое разграничение серверов и пользовательского сегмента сети	Рекомендуемый параметр – пользователи не имеют доступ к серверам
2.	Сетевое разграничение рабочих мест администраторов и пользовательского сегмента сети	Рекомендуемый параметр – рабочие места администраторов отделены от пользовательского сегмента сети – физически или логически (межсетевым экраном, технологией VLAN)
3.	Фильтрация входящего/исходящего сетевого трафика	Рекомендуемый параметр – межсетевой экран фильтрует весь входящий/исходящий в ЛВС трафик (защищены все точки подключения к сети Интернет), правила фильтрации запрещают любой входящий/исходящий трафик, кроме разрешенного (необходимого для выполнения функций органа ПУ). Фильтрация осуществляется по IP– адресам (DNS именам), портам и протоколам.
4.	Совместное использование ресурсов ЛВС со сторонними организациями	Рекомендуемый параметр – ЛВС используется только ее владельцем (сторонние подключения недопустимы)

7. Система антивирусной защиты (проверяется выборочно на серверах и рабочих станциях).

№ п/п	Вопрос проверки	Результат проверки
1.	Наличие антивирусного средства	Рекомендуемый параметр – антивирус установлен
2.	Обновление антивирусного средства	Рекомендуемый параметр – антивирус своевременно обновляется
3.	Проведение антивирусных проверок	Рекомендуемый параметр – проверки проводятся в соответствии с установленной в организационной документации периодичностью
4.	Использование антивирусного средства для проверки входящего трафика	Рекомендуемый параметр – использование как минимум двух антивирусных средств разных производителей (например, потоковый антивирус на точке входа одного производителя и антивирус для почтового сервера (или для файлов, загружаемых в веб– приложения из сети Интернет, и т.п.) другого производителя)

8. Система управления обновлениями программного обеспечения.

№ п/п	Вопрос проверки	Результат проверки
1.	Обновление системного программного обеспечения	Рекомендуемый параметр – использование централизованного обновления сервер обновлений WSUS (для Windows) и RPM–репозитория (для Linux) Рекомендуемый параметр – рабочие станции и серверы должны иметь актуальные обновления безопасности в полном объеме (обязательное тестирование обновлений, сроком не более 2 месяцев)
2.	Обновление прикладного программного обеспечения (браузеры, офисные приложения, архиваторы и т.п.).	Рекомендуемый параметр – все прикладное программное обеспечение должно иметь актуальные версии
3.	Использование устаревшего системного и прикладного программного обеспечения (обновления безопасности не выпускаются)	Рекомендуемый параметр – неподдерживаемое программное обеспечение не должно применяться

9. Система резервного копирования.

№ п/п	Вопрос проверки	Результат проверки
1.	Наличие надежной независимой системы резервного копирования наиболее значимой информации	Рекомендуемый параметр – должна быть настроена и работоспособна система резервного копирования (в виде отдельной или независимой системы). Отдельной системой или независимой системой может являться автоматизированное рабочее место, либо автономная станция хранения данных (NAS – система).
2.	Использование жестких дисков	Рекомендуемый параметр – для хранения резервных копий и критической информации должно быть обеспечено использование жестких дисков не ниже "корпоративного класса" надежности

10. Организационные меры по защите информации в ЛВС.

№ п/п	Вопрос проверки	Результат проверки
1.	Регламентирование контролируемой зоны органа ПУ	Рекомендуемый параметр – в ПУ разработан и утвержден документ, в котором в схематичном виде изображена территория, на которой исключено несанкционированное нахождение посторонних лиц и транспортных средств. Документ актуален и соответствует фактическим условиям функционирования ПУ
2.	Внедрение порядка и "культуры" работы на автоматизированном рабочем месте	Рекомендуемый параметр – – создать официальную политику (документ), устанавливающую запрет на использование неавторизованного программного обеспечения; – создать официальную политику защиты от рисков, связанных с получением файлов и программного обеспечения, либо из внешних сетей, либо через другие передающие среды, показывающую, какие защитные меры следует принять; – проводить регулярный анализ программного обеспечения и

№ п/п	Вопрос проверки	Результат проверки
		содержания данных систем, поддерживающих критические процессы организации; необходима формальная процедура расследования причин наличия любых неавторизованных или измененных файлов;
3.	Регламентирование порядка работы в случае подозрения на наличие вирусного программного обеспечения или ссылок на подозрительные веб– ресурсы ("фишинговые" ссылки) в почтовых сообщениях	Рекомендуемый параметр – порядок регламентирован, в нем указаны основные признаки "спам– писем", описан порядок действий пользователей в случае подозрения на наличие вирусного программного обеспечения в почтовом сообщении, все сотрудники ПУ с порядком ознакомлены
4.	Ограничение использования в служебных целях информационных систем, технические средства которых расположены за пределами Российской Федерации	Рекомендуемые параметры – все сотрудники ПУ ознакомлены с федеральным законом от 27.07.2006 № 149– ФЗ "Об информации, информационных технологиях и о защите информации"
5.	Использование в служебных целях общедоступных почтовых сервисов (mail.ru, yandex.ru и т.п.), предоставляемых юридическими лицами, зарегистрированными на территории Российской Федерации	Рекомендуемый параметр – общедоступные почтовые сервисы не используются
6.	Регламентирование порядка работы с веб– приложениями	Рекомендуемый параметр – сотрудники, ответственные за работу с веб– ресурсами, ознакомлены с правилами антивирусной защиты: 1. Сотрудники должны проводить обязательную предварительную антивирусную проверку файлов, загружаемых на веб– ресурсы внутренними антивирусными средствами; 2. Сотрудники не выполняют административный доступ к веб– приложениям с личных устройств

11. Системы защиты среды виртуализации.

№ п/п	Вопрос проверки	Результат проверки
1.	Разделение доступа к средствам управления среды виртуализации	Рекомендуемый параметр – доступ к средствам управления имеют только те сотрудники, которым это необходимо для исполнения своих должностных обязанностей

12. Система физической безопасности.

№ п/п	Вопрос проверки	Результат проверки
1.	Техническая и организационная реализация пропускного режима	Возможные рекомендуемые параметры – наличие запущенной в эксплуатацию системы управления контролем доступа (действующая система не допускает бесконтрольного нахождения посторонних лиц в пределах контролируемой зоны); – наличие функционирующего бюро пропусков с фиксацией всех посетителей (действующая система не допускает бесконтрольного нахождения посторонних лиц в пределах контролируемой зоны)

№ п/п	Вопрос проверки	Результат проверки
2.	Организация видеонаблюдения	Рекомендуемый параметр – видеонаблюдение создано, система контролирует все точки входа в административное здание и внутренние коридоры (переходы)
2.1.	Физическое размещение системы видеонаблюдения	Рекомендуемый параметр – система видеонаблюдения является автономной (без использования посторонних "облачных" сервисов)
2.2.	Сетевое размещение системы видеонаблюдения	Рекомендуемый параметр – система видеонаблюдения размещена в отдельном сетевом пространстве без подключения к сетям общего пользования (в том числе к сети Интернет). Система видеонаблюдения имеет сервер хранения видеозаписей с установленным сроком их хранения. Хранение видеозаписей осуществляется не менее 7 дней. Межсетевое экранирование организовано таким образом, что доступ к системе видеонаблюдения возможен только для лиц, которым такой доступ необходим для исполнения своих должностных обязанностей
3.	Организационное ограничение возможности физического подключения к ЛВС (в случае отсутствия технической реализации ограничения возможности подключения посторонних устройств к ЛВС)	Возможные рекомендуемые параметры: – в ПУ разработан порядок работы пользователей, в котором регламентирован порядок доступа посторонних лиц в помещения, в которых размещены технические средства ЛВС

Приложение №3
к Методическим рекомендациям оценки
состояния системы защиты
государственных информационных систем
Республики Алтай
и информационно-телекоммуникационной
инфраструктуры исполнительных органов
государственной власти
Республики Алтай на 2022 год

РЕКОМЕНДАЦИИ
по содержанию отчета по результатам тестирования на проникновение контроля

1. Описание методики тестирования на проникновение, включающее в себя:

– условия проведения работ;

– модель нарушителя;

– перечень используемых методологий;

– перечень инструментальных автоматизированных средств;

– оценку уровня критичности уязвимостей.

2. Границы проведения работ (пул тестируемых внешних IP адресов).

3. Описание исследования сетевого периметра, включающее в себя:

– применяемые методы: пассивный сбор информации, анализ собранной информации, активный сбор информации, попытка проникновения;

– перечень сайтов и утилит, используемых для исследования сетевого периметра.

4. Описание идентификации доступных сетевых служб, включающее в себя:

– описание режимов сканирования;

– перечень обнаруженных TCP/UDP служб на каждом обнаруженном узле;

– перечень рекомендаций по настройке сетевых служб, доступных из сети Интернет.

5. Описание инструментального сканирования доступных ресурсов на периметре.

– распределение узлов по максимальному уровню риска обнаруженных на них уязвимостей;

– распределение уязвимостей по степени риска;

– распределение уязвимостей по категориям;

– рейтинг наиболее уязвимых узлов;

– перечень общедоступных эксплойтов (IP– адрес узла – уязвимость по международным классификаторам – ссылка на эксплойт).

– результаты тестирования на проникновение каждого узла в отдельности с указанием его IP– адреса (например, список веб– приложений на узле, графическое отображение (снимки экранов) результатов тестирования на проникновение, результаты атак "подбор пароля" с указанием скомпрометированной учетной записи (логин:пароль).

6. Анализ инцидентов, который должен содержать описание хода оказания услуг (анализ инцидентов) детализированное описание каждого инцидента с его графическим изображением (с учетом IP– адресов и DNS– имен атакованных узлов, времени проведения атак, отображением векторов атак, описание действий, совершаемых во время проведения атаки).

7. Оценка уровня защищенности, состоящую из:

7.1. Оценки общего уровня защищенности, которая должна включать:

– описание привилегий нарушителей, достаточных для:

• получения полного контроля над ИС ИОГВ РА;

• преодоления сетевого периметра и получения доступа во внутреннюю сеть ИОГВ РА.

– описание полученных привилегий от лица внешнего нарушителя;

– максимального уровня критичности обнаруженных уязвимостей;

– максимального уровня критичности обнаруженных уязвимостей, связанных с недостатками конфигурации;

– максимального уровня критичности обнаруженных уязвимостей, устраняемых обновлениями;

– максимального уровня критичности обнаруженных уязвимостей, связанных с ошибками в коде веб– приложений;

– уровня защищенности ИС ИОГВ РА от атак со стороны внешнего нарушителя.

7.2. Оценки уровня защищенности по векторам проникновения, которая должна содержать:

– описание векторов проникновения;

– оценку уровня защищенности по каждому вектору проникновения в отдельности с проставлением оценочных баллов;

– графическое изображение (диаграмма) оценки уровня защищенности по векторам проникновения с отображением текущего уровня защищенности, среднего уровня защищенности и приемлемого уровня защищенности с проставлением оценочных баллов.

7.3. Оценку эффективности механизмов защиты, которая должна содержать:

– оценку эффективности механизмов защиты с проставлением оценочных баллов по видам механизмов защиты:

• сетевая безопасность, в том числе веб– приложений;

• аутентификация и разграничение доступа;

• криптографическая защита;

• управление конфигурациями;

• управление уязвимостями и обновлениями;

- управление учетными записями и паролями;
- антивирусная защита;
- защита среды виртуализации;
- выявление и предотвращение атак.

– графическое изображение (диаграмма) оценки эффективности механизмов защиты с отображением текущего уровня защищенности, среднего уровня защищенности и приемлемого уровня защищенности с проставлением оценочных баллов.

8. Результаты тестирования на проникновение с рекомендациями по устранению выявленных уязвимостей и недостатков.

9. Приложения:

– реестр выявленных уязвимостей, включающий в отношении каждой угрозы:

- уровень риска;
- наименование уязвимости или недостатка механизма безопасности;
- наименование угрозы;
- сложность реализации угрозы;
- описание угрозы;
- рекомендации по устранению выявленных уязвимостей и недостатков механизмов защиты;
- IP– адрес и DNS имя (при наличии) уязвимого ресурса.

– доступные из сети Интернет сетевые службы.